ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

—— ☙(*)❧ ——

Ngô Trung Kiên

BẢO MẬT THÔNG TIN TRONG HỆ THỐNG DI ĐỘNG W- CDMA

KHOÁ LUẬN TỐT NGHIỆP ĐẠI HỌC CHÍNH QUY

Ngành: Điện tử – Viễn Thông

HÀ NỘI - 2005

ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

—ꕥ(*)ꕥ—

Ngô Trung Kiên

BẢO MẬT THÔNG TIN TRONG HỆ THỐNG DI ĐỘNG W- CDMA

KHOÁ LUẬN TỐT NGHIỆP ĐẠI HỌC CHÍNH QUY

Ngành: Điện tử – Viễn Thông

Cán bộ hướng dẫn: PGS.TS. Nguyễn Viết Kính

HÀ NỘI - 2005

LỜI CẢM ƠN

Vấn đề bảo mật và nhận thực ngay từ đầu tuy rất hấp dẫn song cũng là rất khó và đòi hỏi khả năng tính toán cao. Tuy nhiên với nỗ lực làm một khoá luận của một sinh viên chất lượng cao cùng với sự giúp đỡ đặc biệt nhiệt tình của thầy hướng dẫn: PGS.TS. Nguyễn Viết Kính, cùng với sự tận tình chỉ bảo của các thầy trong Khoa Điện Tử - Viễn Thông, các giáo sư nước ngoài thông qua các bộ môn tôi đã được đào tạo thông qua chương trình đại học chính quy và chương trình đào tạo chất lượng cao, cũng như sự giúp đỡ giải quyết các vướng mắc riêng, cùng với sự chỉ bảo tận tình của các thầy thuộc Khoa CNTT trong quá trình mô phỏng tính toán tôi đã dần hiểu mình cần làm những việc gì để hoàn thiện thật tốt khoá luận này cũng như có thể chủ động thực hiện những tính toán thật đầy đủ bằng phần mềm. Bởi vậy thông qua đây tôi xin bày tỏ lòng cảm ơn đến PGS.TS. Nguyễn Viết Kính, các giảng viên thuộc Khoa Điện Tử - Viễn Thông, những người nhiệt tình với kế hoạch đào tạo sinh viên CLC, và cuối cùng là gia đình tôi - những người đã tạo điều kiện hết sức đặc biệt cho cá nhân tôi cả về kiến thức, tài chính, lẫn tinh thần để hoàn thiện khoá luận này. Tôi xin kính chúc mọi người đạt được mọi ước mơ trong cuộc sống.

Sinh Viên CLC

Ngô Trung Kiên.

Tóm tắt nội dung khoá luận

Khoá luận tập trung vào vấn đề đang trở lên ngày càng quan trọng và nóng bỏng hiện nay, vấn đề bảo mật thông tin trong viễn thông. Khoá luận sẽ hướng đối tượng chính vào sự đảm bảo an toàn thông tin trong hệ thống điện thoại di động WCDMA. Qua khoá luận ta sẽ thể thấy được cấu trúc hệ thống và các bộ phận chức năng của hệ thống tham gia vào các quy trình nhận thực, bảo mật.

Khoá luận sẽ tập trung nghiên cứu về quy trình nhận thực, bảo mật thông tin, các bước thực hiện đang và sẽ được dùng trong các quy trình này. Các bước thực hiện sẽ được mô phỏng một cách chi tiết và cụ thể để có thể thấy rõ những ưu điểm và hạn chế của từng biện pháp, từ đó tìm ra hướng phát triển, cải tiến, nghiên cứu tiếp tục nhằm đạt được các phương pháp tối ưu hơn.

Muc luc

Trang

----------o0o----------

Tài liệu tham khảo

Các danh từ viết tắt

Chữ viết tắt	Chữ tiếng Anh	Nghĩa tiếng Việt
A-key	Authentication key	Khoá nhận thực
ASS	Access Switching Subsystem	Phân hệ chuyển mạch truy cập
AUC	Authentication Center	Trung tâm nhận thực
BS	Base Station	Trạm gốc
BSC	Base Station Controller	Bộ điều khiển trạm gốc
BSM	Base Station Manager	Bộ quản lý trạm gốc
BSS	Base Station Subsystem	Phân hệ trạm gốc
BTS	Base station Transceiver Subsystem	Phân hệ phát thu của trạm gốc
CCS	Central Control Subsystem	Phân hệ điều khiển trung tâm
CRC	Cyclic Redundancy Code (CRC)	Mã kiểm tra độ dư thừa vòng
CS	Circuit Switched	Chuyển mạch kênh
EDGE	Enhanced Data Rates for GSM Evolution	Tốc độ số liệu tăng cường để phát triển GSM
ESN	Electronic Serial Number	Số sêri điện tử
ETSI	European Telecommunication Standards Institute	Viện tiêu chuẩn viễn thông châu Âu
FDD	Frequency Division Duplex	Ghép song công phân chia theo tần
FTC	Forward Traffic Channel	Kênh lưu lượng hướng đi
GGSN	Gateway GPRS Support Node	Nút hỗ trợ cổng GPRS
GMSC	Gateway MSC	Cổng MSC
GPRS	General Packet Radio Service	Dịch vụ vô tuyến gói chung
HLR	Home Location Register	Bộ đăng ký thường trú
HSCSD	High Speed Circuit Switched Data	Số liệu chuyển mạch kênh tốc độ cao
IMSI	International Mobile Subscriber Identity	Nhận dạng thuê bao quốc tế

IMT – 2000	International Mobile Telecommunication - 2000	Tiêu chuẩn thông tin di động toàn cầu 2000
IS-136	Interim Standard -136	Chuẩn TDMA cải tiến của USA
ISN	Interconnection Network Subsystem	Phân hệ liên kết mạng
ITU – R	International Telecommunication Union Radio sector	Liên minh viễn thông quốc tế bộ phận vô tuyến
IWF	Interworking Function	Chức năng kết nối mạng
LPC	Linear Predictive Coder	Bộ mã hoá dự đoán tuyến tính
MCC	Mobile Country Code	Mã nước di động
MNC	Mobile Network Code	Mã mạng di động
MS	Mobile Station	Trạm di động
MSC	Mobile Switching Center	Trung tâm chuyển mạch di động
MSIN	Mobile Station Identification Number	Chỉ số nhận dạng trạm di động
MT	Mobile Terminated	Kết cuối ở MS
MX	Mobile Exchange	Tổng đài di động
NMSI	National Mobile Station Identify	Nhận dạng di động quốc gia
NMT	Nordic Telegraph and Telephone	Điện báo và điện thoại Bắc Âu
PCS	Personal Communication Services	Hệ thống các dịch vụ thông tin cá nhân
PDN	Public Data Network	Mạng dữ liệu công cộng
PDGN	Packet Data Gateway Node	Nút cổng dữ liệu gói
PDSN	Packet Data Serving Node	Nút dịch vụ dữ liệu gói
PS	Packet Switched	Chuyển mạch gói
SCP	Service Control Point	Điểm điều khiển dịch vụ
SHA	Secure Hashing Algorithm	Thuật toán băm có bảo mật
SIM	Subscriber Identity Module	Mô đun nhận dạng thuê bao
SSD	Shared Secret Data	Số liệu bí mật chung
TACS	Total Access Communication System	Hệ thống truy nhập toàn bộ
TAF	Terminal Adaptation Function	Chức năng kết cuối thích nghi

TDD	Time Division Duplex	Ghép song công phân chia theo thời gian
TIA	Telecommunication Industry Association	Hiệp hội các nhà sản xuất viễn thông
TMSI	Temporary Mobile Subscriber Identity	Nhận dạng thuê bao di động tạm thời
RAND	Random challenge Memory	Bộ nhớ hiệu lệnh ngẫu nhiên
RIC	Reverse Information Channel	Kênh thông tin hướng ngược
RNC	Radio Network Controller	Bộ điều khiển mạng vô tuyến
RNS	Radio Network Subsystem	Hệ thống con mạng vô tuyến
RSC	Reverse Signaling Channel	Kênh báo hiệu hướng ngược
RTT	Radio Transmission Technology	Kỹ thuật truyền dẫn vô tuyến
UIM	User Identity Module	Mô đun nhận dạng người dùng
UMTS	Universal Mobile Telecommunication System	Hệ thông thông tin di động toàn cầu
VLR	Visitor Location Register	Bộ đăng ký tạm trú
VLR/GLR	Visitor/Gateway Location Register	Bộ đăng ký tạm trú/cổng
WAP	Wireless Application Protocol	Giao thức ứng dụng không dây
WCDMA	Wideband Code Division Multiple Access	Đa truy nhập phân chia theo mã băng rộng

Chương 1: Mở đầu

1.1. Khái niệm

Nhận thực - bảo mật là khái niệm bao gồm tất cả các phương pháp như các kỹ thuật xác nhận danh tính, mật mã hoá, che giấu thông tin, xáo trộn … nhằm đảm bảo cho các thông tin được truyền đi, cũng như các thông tin lưu trữ được chính xác và an toàn.

1.2. Sự cần thiết của bảo mật

Ngay từ thời xa xưa, khoảng 4000 năm về trước để tỏ lòng tôn kính người đã khuất, người Ai Cập đã khắc những mã hiệu tượng hình nên các bia mộ. Các mã hiệu mật được khắc trong các ngôi mộ cổ cho đến ngày nay vẫn được các nhà khảo cổ tìm hiểu khám phá. Qua các thời kỳ, cùng với thời gian, kỹ thuật mật mã hoá đã có nhiều thay đổi và ngày càng hoàn thiện. Trong chính trị, quân sự, cũng như trong kinh tế, thời chiến cũng như thời bình, thì sự bảo mật thông tin và an toàn thông tin là vấn đề ưu tiên hàng đầu. Sự bảo đảm an toàn thông tin hầu như tuyệt đối là đòi hỏi đầu tiên đối với truyền thông trong các lĩnh vực quan trọng. Chúng ta đã thấy vai trò cực kỳ quan trọng của nó không chỉ trong chiến tranh Việt Nam mà bất kỳ một cuộc chiến nào, từ thời xa xưa với cuộc chiến giữa các tộc người đến thời kỳ hiện đại với các cuộc chiến tranh của thời đại nguyên tử, từ các cuộc nội chiến với quy mô nhỏ, đến các cuộc thế chiến quyết định tính mạng của toàn nhân loại.

Ngày nay sự bảo đảm an toàn thông tin đã trở thành vấn đề quan tâm của rất nhiều người trong đó có các cá nhân, các tổ chức, cũng như các chính phủ, khi mà nguy cơ đe doạ bị rò rỉ tin tức hoặc nguy cơ bị xâm nhập đang trở thành vấn đề phải đối phó hàng ngày, hàng giờ.

Các chính phủ đã bỏ ra nhiều triệu đô la để có được một hệ thống viễn thông an toàn, các công ty hoặc các cá nhân giàu có cũng đã mất rất nhiều tiền bạc để đầu tư cho sự an toàn về tin tức của họ, ngay cả các cá nhân bình thường hiện tại cũng chẳng muốn có ai đó biết được những bí mật riêng của mình. Do đó vấn đề bảo đảm tuyệt đối an toàn cho các cá nhân, tổ chức sử dụng dịch vụ viễn thông là nhiệm vụ của những nhà cung cấp dịch vụ, hệ thống nào mà có độ an toàn càng cao, thì sẽ càng có khả năng cạnh tranh trong thời đại ngày nay.

Công nghệ viễn thông trong những năm gần đây đã có những bước tiến nhảy vọt và có vai trò ngày càng quan trọng đối với xã hội, trong đó thông tin di động ngày càng được phát triển và mở rộng ra nhiều dịch vụ, song song với nó là nhu cầu của

người sử dụng cũng không ngừng nâng cao, yêu cầu này chủ yếu là các dịch vụ phong phú, tốc độ cao. Đối với các cuộc trao đổi thông tin mang tính riêng tư, kinh doanh, chứng khoán, thị trường … ngoài đòi hỏi các yêu cầu trên ra, còn đòi hỏi vừa phải mang tính chính xác (ở nơi thu sẽ thu được đúng những gì mà bên phát đã gửi đi) vừa phải mang tính bảo mật (giữ kín những gì đã gửi đi) không cho các đối thủ cạnh tranh trong kinh doanh có thể dò ra được để có thể sử dụng hoặc phá hoại thông tin đó. Vấn đề này càng quan trọng đối với các thông tin liên quan đến an ninh quốc gia, chúng ta thường nghe đến các khái niệm: bí mật quốc gia, tình báo chính trị, tình báo kinh tế, thiết bị do thám… và biết được mức độ quan trọng của nó đối với sự thịnh vượng, chủ quyền của một đất nước. Tất cả những điều đó chứng tỏ bí mật thông tin là yếu tố sống còn đối với một quốc gia, một xã hội.

Các vụ kiện cáo trong kinh doanh, ngân hàng liên quan đến vấn đề xác nhận đã gửi, đã nhận rất có thể sẽ không tránh khỏi nếu như xử lý vấn đề này không tốt. Ví dụ như trong kinh doanh bên A đã gửi một bản tin (chẳng hạn như một hợp đồng) cho bên B, có thể xảy ra các trường hợp sau:

+ Bên B đã nhận được bản tin đó, nhưng khi thực hiện có trục trặc gây bất lợi cho bên B, thì rất có thể bên B sẽ cố ý bác bỏ là đã nhận được tin nhắn mà bên A đã gửi.

+ Ngược lại khi mà A đã gửi bản tin nhưng lại nhận thấy rằng nếu bên B nhận được bản tin đó sẽ gây bất lợi cho mình thì bên A có thể bác bỏ rằng họ đã không gửi bản tin đó mà có thể bên B nhận được bản tin đó từ kẻ phá hoại nào đó (mà bên A cố tình tưởng tượng ra).

Để đảm bảo an toàn thì một bản tin nhận được phải đạt được các yêu cầu sau:

- Thông báo được bắt đầu với người gửi có chủ đích
- Nội dung thông báo không được thay đổi
- Thông báo được nhận theo trình tự mà người khởi đầu cuộc liên lạc đã gửi nó

Chính vì vậy mà cần có một phương pháp nào đó để trước toà bên A phải thừa nhận rằng mình đã gửi bản tin đó, và bên B cũng phải thừa nhận rằng mình đã nhận được bản tin đó từ bên A.

Trường hợp thường gặp nữa là lỗi không phải do bên A hay bên B cố tình chối cãi, mà có kẻ thứ ba phá hoại giả là bên A gửi bản tin cho bên B (hoặc giả làm bên B để nhận thông báo từ bên A), trường hợp này mạng phải có thể nhận biết được bản tin đó không phải là từ bên A mà từ một kẻ khác để cảnh báo cho bên B .

Chính vì vậy xác thực một thông báo sẽ liên quan đến xác nhận danh tính của người gửi và người nhận, tới sự phát hiện những biến đổi nội dung thông báo, và phát hiện sự quay lại (phát lặp lại). Những thay đổi không mong muốn có thể là do điều kiện khách quan, chẳng hạn như tạp âm trên kênh truyền, hoặc có thể là do sự ác ý của nhóm thứ 3.

Trong thông tin nói chung bảo mật đã rất quan trọng như vậy, mà như chúng ta đã biết môi trường truyền tin của thông tin di động là môi trường truyền dẫn vô tuyến (môi trường hở) - môi trường rất dễ bị nghe trộm và sử dụng trộm đường truyền, ví dụ như là hệ thống thông tin di động sử dụng kỹ thuật FDMA chỉ cần biết được giải tần làm việc, khuôn dạng khung truyền ta có thể dễ dàng thu được cuộc trao đổi trên đường truyền giống như thu sóng Radio thông thường.Việc sử dụng trộm đường truyền này làm cho tiền cước phải trả của thuê bao bị lợi dụng tăng cao là một nguy cơ không thể tránh khỏi.

Bảo vệ quyền lợi của thuê bao, và bảo vệ bí mật dữ liệu trên mạng cho thuê bao cần phải có những biện pháp đặc biệt để đảm bảo rằng khi truy cập chỉ có thể là máy của thuê bao và dữ liệu gửi đi chỉ có thể là của thuê bao nhất định và đó là thiết bị duy nhất, đồng thời dữ liệu đó chỉ đến đích cần gửi và chỉ có đích cần nhận mới hiểu đó là cái gì, tất cả các kỹ thuật đó gọi là kỹ thuật bảo đảm an toàn thông tin. Để đảm bảo quyền lợi của người thuê bao cần giữ bí mật số nhận dạng thuê bao, và kiểm tra tính hợp lệ của người sử dụng khi họ truy nhập mạng. Để chống nghe trộm cần mật mã hoá thông tin của người sử dụng. Trong thực tế ta gặp rất nhiều phương pháp bảo mật và nhận dạng khác nhau. Trong hệ thống thông tin di động mỗi người có một khoá nhận dạng bí mật riêng được lưu trữ ở bộ nhớ an toàn.

Tất cả các vấn đề trên có thể giải quyết được bằng cách gắn cho mỗi thiết bị đầu cuối một cơ sở dữ liệu duy nhất để mạng có thể biết được chính xác nó đang phục vụ thiết bị đầu cuối nào, và các đầu cuối này sẽ được một người có đủ quyền hạn sử dụng.

Cũng cần phải lưu ý rằng tất cả các phương pháp bảo mật đều có thể bị khám phá và bị khai thác, các nhà cung cấp dịch vụ và các kỹ thuật mới đang nỗ lực tìm các phương pháp để ngăn ngừa sự phá hoại nguy hiểm này. Bởi vì mục đích của chúng ta là đáp ứng các yêu cầu của khách hàng ngày càng tốt hơn, bên cạnh mục tiêu nhanh hơn, rẻ hơn, tiết kiệm hơn, nhiều hơn còn có mục tiêu vô cùng quan trọng đó là tin cậy hơn.Vì những lý do trên việc chúng ta thúc đẩy sự tìm hiểu về vấn đề này là hướng đi đúng đắn vì nó không đòi hỏi phải có vốn lớn mà chỉ cần tư duy, tìm tòi để đưa ra các phương pháp tính toán hiệu quả là chúng ta đã gặt hái được kết quả, điều này rất phù

hợp với khả năng của chúng ta, và nhắc lại một lần nữa rằng nhu cầu này không bao giờ có giới hạn, một thuật toán nào đó dù có tinh vi, phức tạp đến đâu, theo thời gian nhất định sẽ có kẻ tìm ra, và điều đó là cực kỳ mau lẹ trong thời đại thông tin là tiền bạc như hiện nay.

Như vậy vấn đề an toàn thông tin là một vấn đề rất hay cần được xem xét và có hướng phát triển song song với sự phát triển của các kỹ thuật hiện đại. Hiện nay trong lĩnh vực thông tin vô tuyến, thông tin di động đang chuyển từ thế hệ thứ hai (2G) sang thế hệ thứ ba (3G). Để góp phần làm rõ thêm về một số mục tiêu và cách thức bảo đảm bí mật trong thông tin, và cũng để chuẩn bị các kiến thức để tiếp cận với công nghệ mới này chúng ta hãy tìm hiểu các cách thức nhận thực và bảo mật thông tin trong W-CDMA.

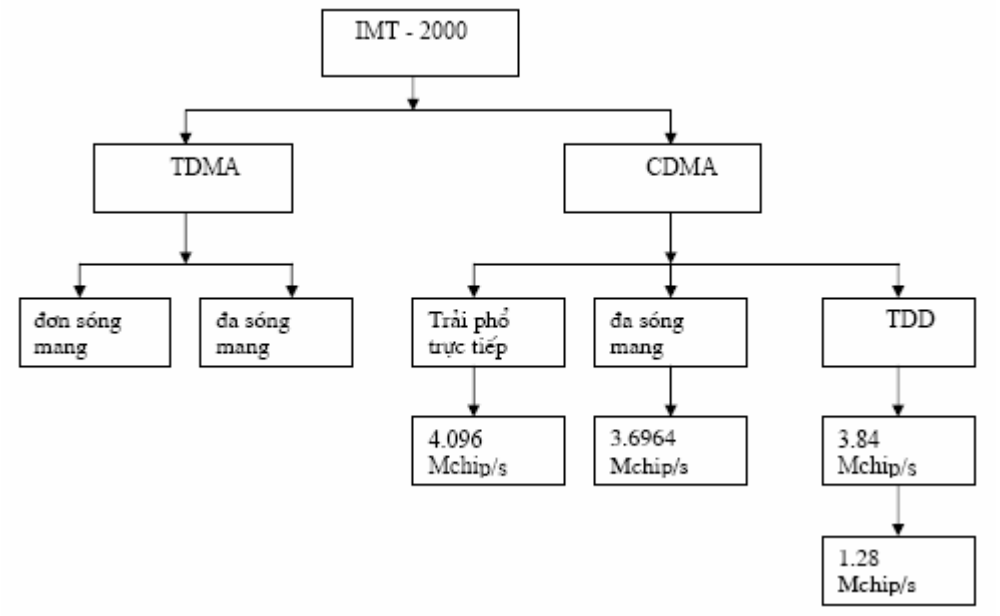
Chương 2: Hệ thống thông tin di động WCDMA

Trước khi vào vấn đề chính, chúng ta hãy bắt đầu bằng việc tìm hiểu hệ thống mà chúng ta cần khảo sát – hệ thống WCDMA.

2.1. Lộ trình phát triển của hệ thống thông tin di động thế hệ thứ 3

Thông tin di động thế hệ hai mặc dù sử dụng công nghệ số nhưng vì là hệ thống băng hẹp và được xây dựng trên cơ chế chuyển mạch kênh nên không đáp ứng được nhu cầu của các dịch vụ mới, thêm vào đó là có quá nhiều tiêu chuẩn khác nhau làm cho việc di chuyển của thuê bao giữa các quốc gia này với quốc gia khác gặp rất nhiều khó khăn. Chính vì lẽ đó mà các tổ chức viễn thông trên thế giới thấy cần thiết phải tập hợp lại và đề ra phương án phải có một tiêu chuẩn thống nhất chung để các hệ thống viễn thông di động tương lai vừa đáp ứng được các yêu cầu của thời đại mới, vừa mang tính thống nhất chung cho các hệ thống. Kết quả là IMT – 2000 do ITU – R xây dựng đã ra đời nhằm đáp ứng yêu cầu của thế kỷ XXI. IMT - 2000 mở rộng đáng kể khả năng cung cấp dịch vụ và cho phép nhiều phương tiện thông tin có thể cùng hoạt động, từ các phương tiện truyền thống cho đến các phương tiện hiện đại và các phương tiện truyền thông sẽ có trong tương lai.

Trong tiêu chuẩn IMT – 2000 các phân hệ của thông tin di động được chia như sau:



Hình 2.1. Phân hệ tiêu chuẩn quốc tế IMT- 2000

Theo chuẩn trên thì:

WCDMA – CDMA trải phổ trực tiếp

CDMA2000 – CDMA đa sóng mang.

Lộ trình tiến lên WCDMA từ GSM

Lộ trình đó được miêu tả như sau:

HSCSD: High Speed Circuit Switched Data: Số liệu chuyển mạch kênh tốc độ cao

GPRS: General Packet Radio Service: Dịch vụ vô tuyến gói chung

EDGE: Enhanced Data Rates for GSM Evolution:

Tốc độ số liệu tăng cường để phát triển GSM

Hình 2.2. Lộ trình từ GSM tiến lên WCDMA

WCDMA là giai đoạn phát triển cuối cùng của ITM – 2000 thuộc lộ trình của hệ GSM tăng cường hỗ trợ các dịch vụ tốc độ cao (ở ô picro tốc độ có thể đặt được 2 Mbps và ở ô macro tốc độ đảm bảo 144 Kbps) và có các tính chất:

- Hoạt động ở CDMA băng rộng với băng tần 5 Mhz
- Lớp vật lý linh hoạt sao cho có thể tích hợp được tất cả các tốc độ trên một sóng mang, từ các tốc độ thấp để đáp ứng các dịch vụ truyền thống như thoại đến các dịch vụ yêu cầu tốc độ cao như VOD (Video On Demand), Internet tốc độ cao

Ngoài ra công nghệ này có tính năng tăng cường sau:

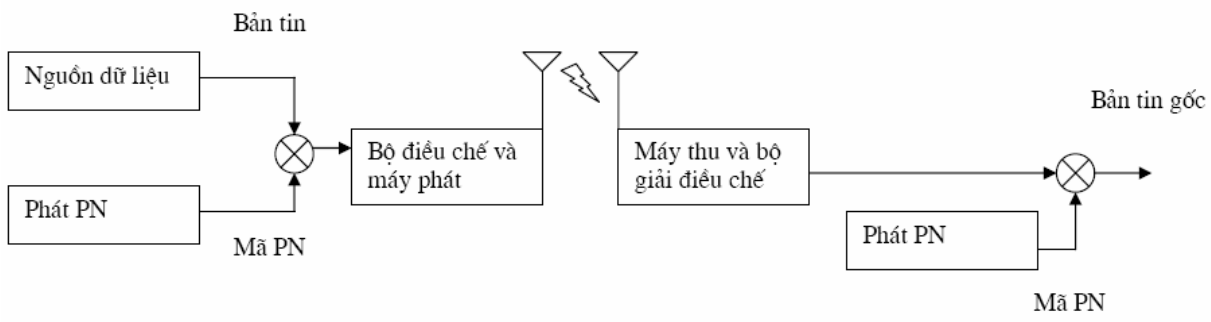
- Phân tập phát
- Anten thích nghi
- Hỗ trợ các cấu trúc thu tiên tiến

Hiện nay ở Việt Nam GPC và VMS đang khai thác hai mạng thông tin di động VinaPhone và MobiFone và một số công ty khác như Viettel… cũng đang tiến hành triển khai dịch vụ với công nghệ theo tiêu chuẩn GSM. Các công ty này đã có những chuyển biến về mặt công nghệ nhằm đáp ứng nhu cầu mới của khách hàng nhất là các

dịch vụ truyền số liệu. Các công ty khai thác đang nghiên cứu chuyển dần sang thông tin di động thế hệ thứ ba. Trước mắt các công nghệ thông tin di động thế hệ 2.5 được đưa vào sử dụng, hai nhà khai thác VinaPhone và MobiFone đã đưa vào mạng của họ công nghệ WAP và GPRS, với công nghệ này làm cho dung lượng truy nhập lên đến 144 Kbps và có thể cho phép truy nhập trực tiếp vào Internet.

2.2. Nguyên lý trải phổ

WCDMA hoạt động trên nguyên lý trải phổ băng rộng nên trước hết chúng ta xem xét nguyên lý trải phổ CDMA.Nguyên lý trải phổ hoạt động theo sơ đồ sau:



Hình 2.3. Nguyên lý phát và thu CDMA

Trong đó: ⊗ : phép XOR

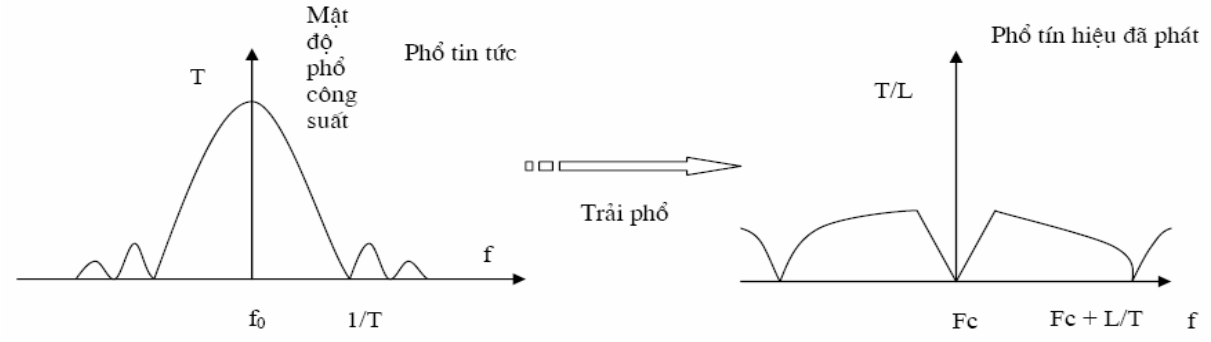
Chu kỳ tín hiệu gốc: T

Chu kỳ mã PN: T/L

Khai triển Fourier: F (∏ (t/ℑ)) = ℑ sinc (Ωℑ/2∏)

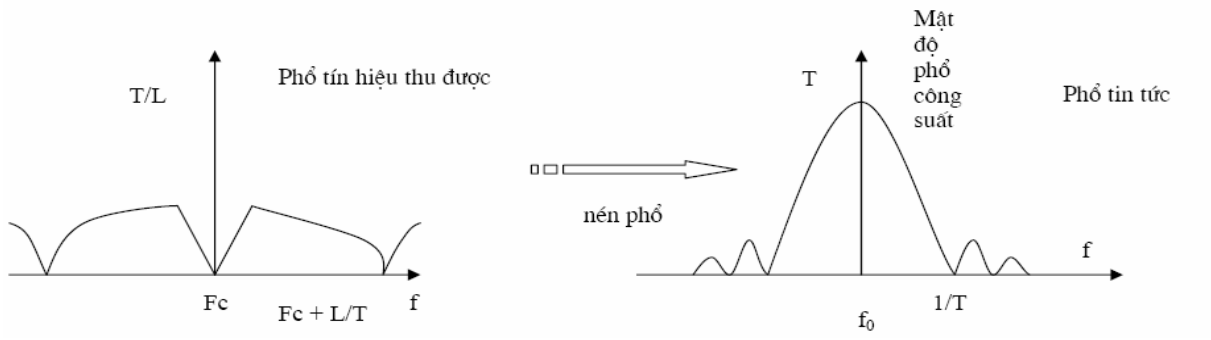
Khảo sát phổ của đầu thu và đầu phát:

Máy phát dùng mã PN để thực hiện trải phổ



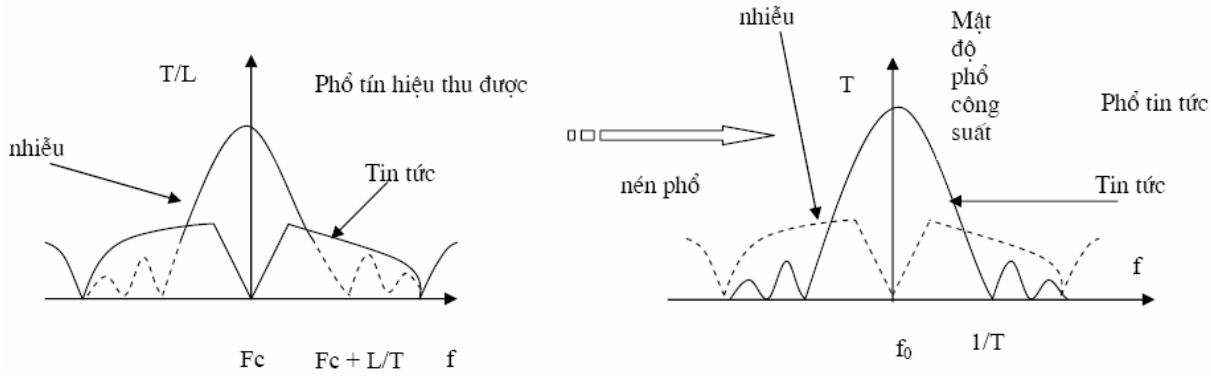
Hình 2.4a. Quá trình trải phổ

Máy thu bản sao của mã PN để nén phổ:



Hình 2.4 b. Quá trình nén phổ

Khi có nhiễu: phổ tín hiệu đã trải phổ được nén lại, phổ nhiễu do chưa được trải phổ sẽ bị dãn ra như hình sau:



Hình 2.4 c. Nén phổ khi có nhiễu

Các tần số f_0 và f_c tương ứng với nguồn tin, sóng vô tuyến (hay cao tần)

CDMA sử dụng kỹ thuật trải phổ nên nhiều người có thể sử dụng cùng một kênh vô tuyến đồng thời khi tiến hành các cuộc gọi. Những người sử dụng này được phân biệt với nhau nhờ một mã đặc trưng không trùng với bất kỳ ai. Kênh vô tuyến CDMA được dùng lại ở mỗi cell trong toàn mạng và các kênh này cũng được phân biệt nhau nhờ mã trải phổ giả ngẫu nhiên.

Để nén phổ ngược trở lại dữ liệu gốc, thì máy thu phải dùng mã trải phổ PN chính xác như khi tín hiệu được xử lý ở máy phát. Nếu mã PN ở máy thu khác hoặc không đồng bộ với mã PN ở máy phát, thì tin tức không thể thu nhận hoặc hiểu được ở máy thu. Rõ ràng tốc độ chip sẽ ảnh hưởng đến sự trải rộng phổ của tín hiệu gốc, chính căn cứ vào đây ta có thể điều chỉnh được độ rộng phổ của tín hiệu trải ra. Tạp âm nền có phổ rộng sẽ bị giảm nhỏ do bộ lọc phát ở máy thu, sau khi nén phổ nhiễu từ các máy thu di động khác sẽ không được nén phổ tương tự như tạp âm. Nhiễu từ các nguồn phát sóng không được trải phổ nếu có băng tần trùng với băng tần của tín hiệu đã được trải phổ thì tại máy thu lập tức sẽ bị trải phổ sau khi thực hiện phép XOR với mã PN,

mật độ phổ công suất của nhiễu này giảm xuống và ta dễ dàng có thể loại bỏ nó bằng cách lấy mức tối thiểu (định mức) tín hiệu.

2.3. *Các đặc tính cơ bản của hệ thống thông tin di động WCDMA*

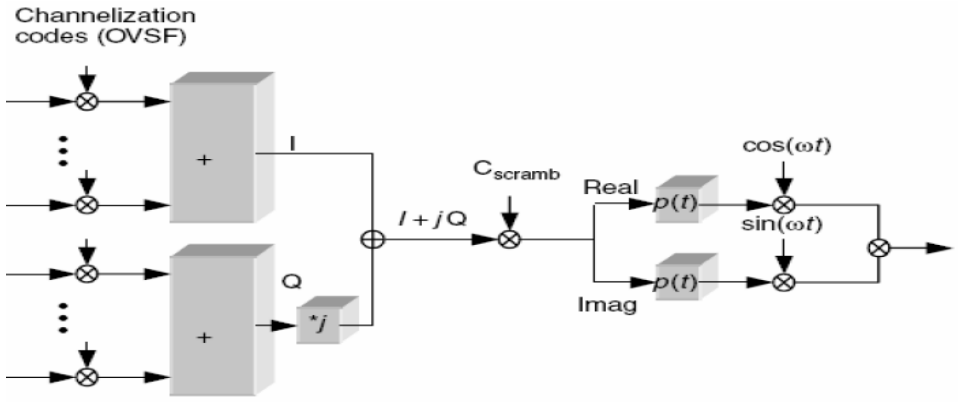
Lớp vật lý của WCDMA do sử dụng công nghệ CDMA nên rất khác so với lớp vật lý của GSM và GPRS. Ngoài ra tổ chức các kênh ở lớp này cũng phức tạp hơn tổ chức các kênh ở thế hệ hai (2G) rất nhiều.

- ***Trải phổ, ngẫu nhiên, điều chế trực giao***

WCDMA sử dụng trải phổ ở tốc độ chip 4.096 Mchip/s. Một hệ thống thông tin di động ngoài việc phân biệt các MS còn phải phân biệt các kênh vật lý, các BTS. WCDMA thực hiện yêu cầu này bằng trải phổ và ngẫu nhiên hoá. Trước hết các kênh khác nhau của BTS được trải phổ bằng mã định kênh ở tốc độ chip 4.096 Mchip/s. Sau đó các kênh này được kết hợp với nhau ở bộ cộng tuyến tính và sau đó được ngẫu nhiên hoá bằng một mã ngẫu nhiên, mã ngẫu nhiên hoá phải có cùng tốc độ chip 4.096 Mchip/s và được dành riêng cho từng BTS.

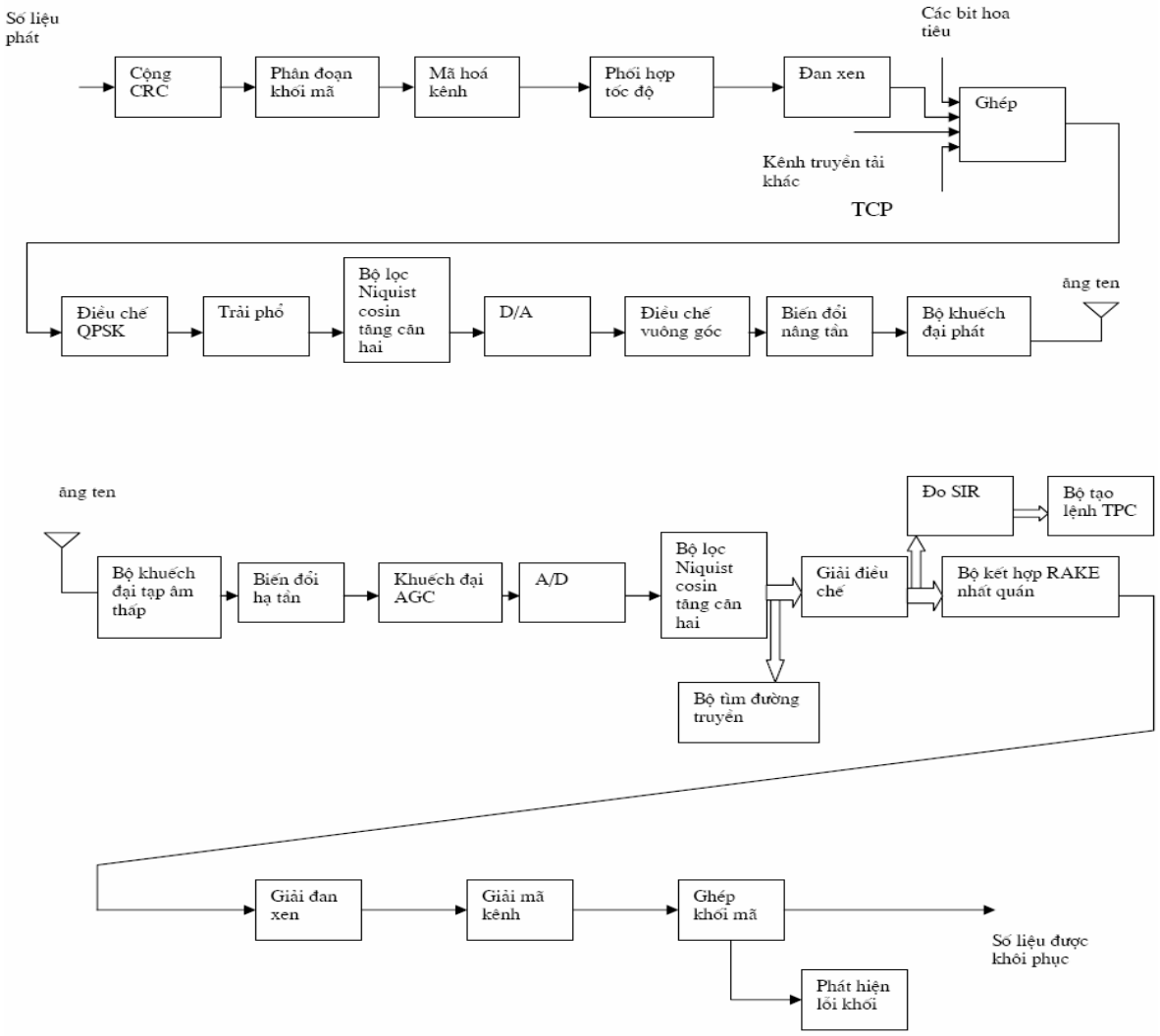
Mã định kênh trải luồng tín hiệu kênh kênh nên làm tăng độ rộng băng tần, còn mã ngẫu nhiên hoá có cùng tốc độ chip thực hiện ngẫu nhiên hoá sau trải phổ nên không làm tăng độ rộng băng tần. Tại đầu thu, trước tiên kênh tín hiệu được giải ngẫu nhiên hoá bằng mã tương ứng với MS hoặc BTS, sau đó các luồng tín số kênh được đưa qua các bộ giải trải phổ bằng các mã định kênh tương ứng để thu được tín hiệu gốc. Như vậy nhiều người có thể sử dụng chung các mã định kênh, và tất nhiên với các mã định kênh khác nhau ta cũng có thể sử dụng lại các mã ngẫu nhiên hoá.

Sau khi được trải phổ và ngẫu nhiên hoá tín hiệu được điều chế trực giao theo sơ đồ nguyên lý sau:



Hình 2.5. Sơ đồ thực hiện trải phổ, ngẫu nhiên hoá và điều chế trực giao

➢ ***Các bước thực hiện khi thu và phát***



Hình 2.6 Sơ đồ khối phát vô tuyến và thu vô tuyến

- Tại bên phát:

Ban đầu tín hiệu được bổ xung mã kiểm lỗi CRC cho từng khối truyền tải TB (Transport Block). Sau đó dữ liệu được mã hoá kênh và đan xen. Số liệu sau đan xen được bổ xung các bit hoa tiêu và bit điều khiển công suất phát (TCP: Transmit Power Control), sau đó được sắp xếp lên các nhánh I và Q của QPSK rồi được trải phổ hai lớp (trải phổ và ngẫu nhiên hoá). Chuỗi bit sau khi ngẫu nhiên hoá được giới hạn trong bộ lọc Niquist cosin tăng căn hai (hệ số dốc bằng 0.22) và được biến đổi thành tương tự bằng bộ biến đổi D/A để đưa lên điều chế vuông góc cho sóng mang. Tín hiệu trung tần (IF) sau điều chế được nâng tần lên sóng vô tuyến (RF) trong băng tần 2 Ghz, sau đó được khuếch đại trước khi chuyển đến anten để phát vào không gian

- Tại phía thu:

Tín hiệu thu được khuếch đại bằng bộ khuếch đại tạp âm nhỏ, sau đó được đưa xuống trung tần (IF) thu rồi được khuếch đại tuyến tính bởi bộ khuếch đại AGC (Automatic Gain Control: Tự điều khiển khuếch đại). Sau khuếch đại AGC, tín hiệu được giải điều chế để được các thành phần I và Q. Các tín hiệu tương tự của các thành phần này được biến đổi thành số ở bộ biến đổi tương tự số A/D, sau đó tín hiệu được cho qua bộ lọc Niquist cosin tăng căn hai và được phân chia theo thời gian vào một số thành phần đường truyền có các thời gian trễ truyền sóng khác nhau. Sau giải trải phổ cho các thành phần này, chúng được kết hợp bởi bộ kết hợp máy thu RAKE, tín hiệu tổng được giải đan xen, giải mã kênh (giải mã sửa lỗi), được phân thành các khối truyền tải TB và được phát hiện lỗi.

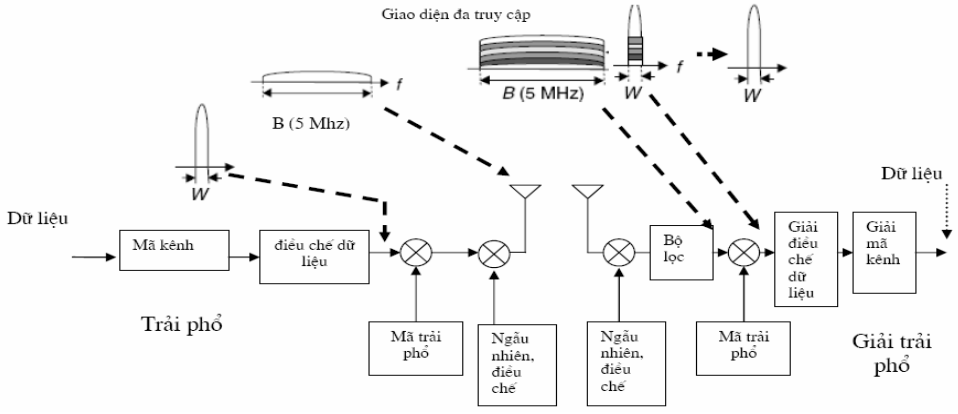
- ***Các giao diện vật lý***

WCDMA có thể có 2 giải pháp cho giao diện vô tuyến: ghép song công phân chia theo tần số (FDD) và ghép song công phân chia theo thời gian (TDD). Cả hai giao diện này đều sử dụng trải phổ trực tiếp (DS - CDMA). Giải pháp thứ nhất được sử dụng rộng dãi còn giải pháp thứ hai chủ yếu được triển khai cho các ô nhỏ (micro và pico).

Giải pháp FDD sử dụng hai băng tần 5 Mhz và hai sóng mang phân cách nhau 190 Mhz đường lên nằm trong dải phổ 1920 Mhz – 1980 Mhz, đường xuống nằm trong giải tần 2110 – 2170 Mhz. Mặc dù 5 Mhz là độ rộng băng tần danh định, ta cũng có thể chọn băng tần từ 4.4 Mhz – 5 Mhz với các nấc 200 Khz. Việc chọn độ rộng băng đúng cho phép ta tránh được nhiễu giao thoa nhất là khi băng tần 5 Mhz tiếp theo thuộc nhà khai thác khác.

Giải pháp TDD sử dụng các tần số nằm trong giải 1900 – 1920 Mhz và từ 2010 – 2025 Mhz ở đây đường lên và đường xuống sử dụng chung một băng tần (không cách nhau như ở FDD).

Thực hiện trải phổ trong hệ thống WCDMA được thực hiện theo sơ đồ sau:



Hình 2.7 Sơ đồ thực hiện phát và nhận ở hệ thống WCDMA

➢ ***Sơ đồ mạng WCDMA và các chức năng cơ bản***

Giao diện vô tuyến của WCDMA hoàn toàn khác với GSM và GPRS, WCDMA sử dụng phương thức trải phổ trực tiếp với tốc độ chip (hay tốc độ cắt) là 4.096 Mcps. Trong WCDMA mạng truy nhập vô tuyến được gọi là mạng UTRAN (UTRAN Terrestrial Radio Access Network). Các phần tử của UTRAN rất khác so với các phần tử của mạng truy nhập vô tuyến của GSM. Vì thế khả năng sử dụng lại các cơ sở vật chất khác như BTS và BSC của GSM là rất hạn chế. Một số nhà sản xuất cũng đã có kế hoạch nâng cấp các BTS của GSM cho WCDMA. Đối với các nhà sản xuất này chỉ có thể tháo ra một số bộ phận thu phát của GSM từ BTS và thay vào đó các bộ thu phát mới cho WCDMA. Một số ít các nhà sản xuất còn lập kế hoạch xa hơn. Họ chế tạo các BSC đồng thời cho cả GSM và WCDMA. Tuy nhiên đa phần các nhà sản xuất phải thay thế BSC trong GSM bằng RNC (bộ điều khiển mạng vô tuyến) mới cho WCDMA.

WCDMA sử dụng rất nhiều kiến trúc của mạng GSM, GPRS hiện có cho mạng của mình, đặc biệt các phần tử như MSC, HLR, SGSN, GGSN có thể được nâng cấp từ mạng hiện có để đồng thời hỗ trợ cả WCDMA và GSM.

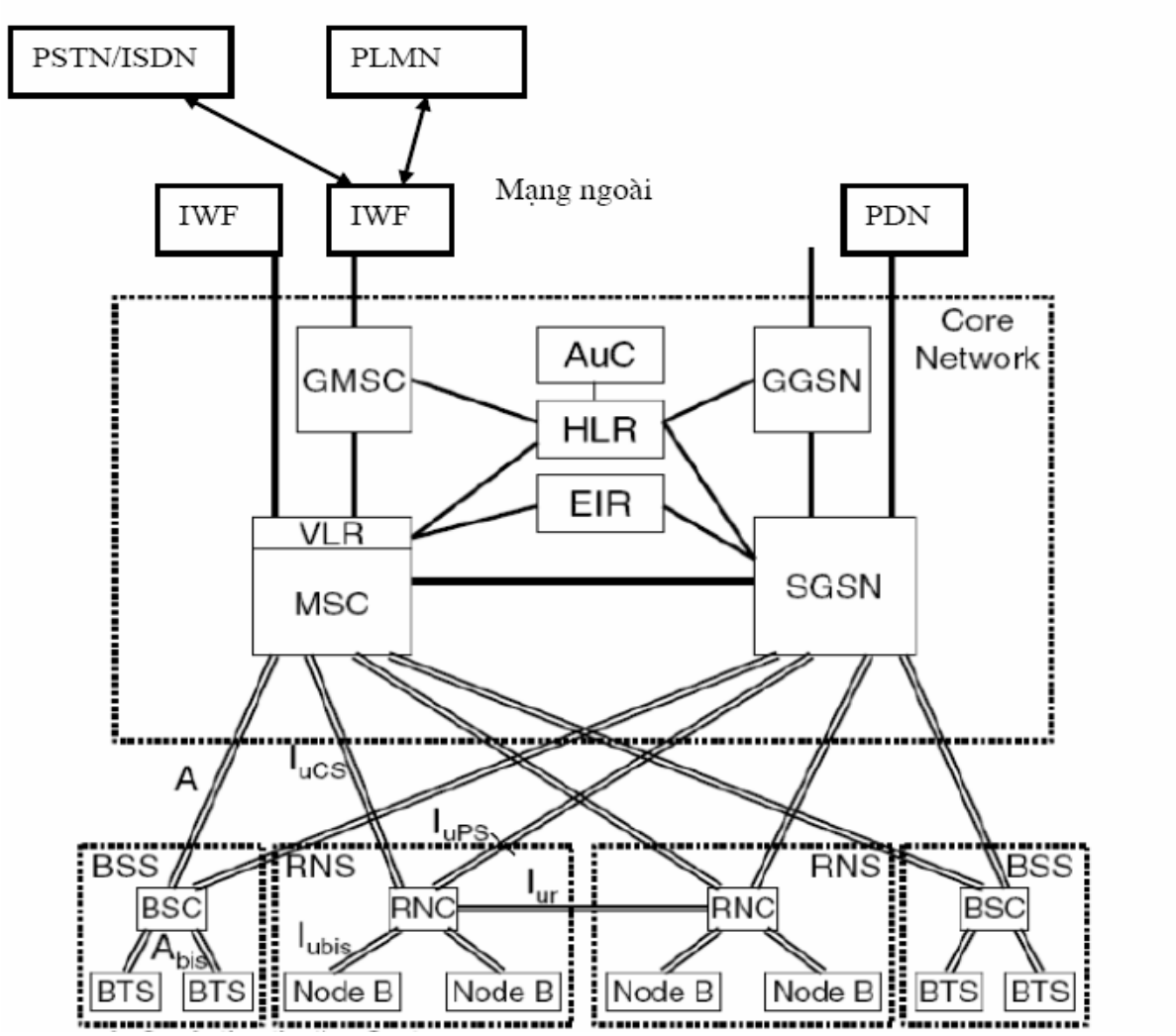
Mạng thông tin di động thế hệ thứ ba (3G) bao gồm hai phần mạng: mạng lõi và mạng truy nhập vô tuyến.

❖ *Mạng lõi*: bao gồm trung tâm chuyển mạch di động (MSC: Mobile Switching Center) và các nút hỗ trợ chuyển mạch gói (SGSN: Serving General packet radio Service support Note). Các kênh thoại và truyền số liệu chuyển mạch gói được kết nối với mạng ngoài qua các trung tâm chuyển mạch di động và nút chuyển mạch gói cổng GMSC và GGSN. Để kết nối trung tâm chuyển mạch di động với mạng ngoài cần có thêm phần tử làm chức năng tương tác mạng (IWF). Ngoài các trung tâm chuyển mạch kênh và các nút chuyển mạch gói mạng lõi còn có chứa các cơ sở dữ liệu cần thiết cho các máy di động HLR, AUC, và EIR.

- EIR: Equipment Identity Register: Bộ ghi nhận dạng thiết bị

Thực hiện việc lưu trữ tạm thời các thông tin liên quan đến các MS đang chịu sự quản lý của mạng để có thể nhận dạng MS khi có khởi xướng gọi hay khi MS bị tìm gọi, hay nói cách khác EIR đóng vai trò như VLR trong GSM , chứa đựng tạm thời thông tin khách hàng khi họ chuyển vùng sang nơi quản lý của MSC khác, các EIR được kết nối với nhau, khi một thuê bao chuyển vùng EIR ở đó sẽ gửi thông tin về

HLR của họ để biết họ ở đâu khi có một cuộc gọi đến họ hoặc khởi phát từ thuê bao đó.



Hình 2.8 Cấu trúc hệ thống mạng WCDMA

- AUC Authentication Center: Trung tâm nhận thực

Là cơ sở dữ liệu được bảo vệ nghiêm ngặt. Sử lý mật mã và nhận thực khách hàng khi đối chiếu với cơ sở dữ liệu gốc. Thực hiện quản lý thuê bao, bao gồm các hoạt động quản lý đăng ký thuê bao.

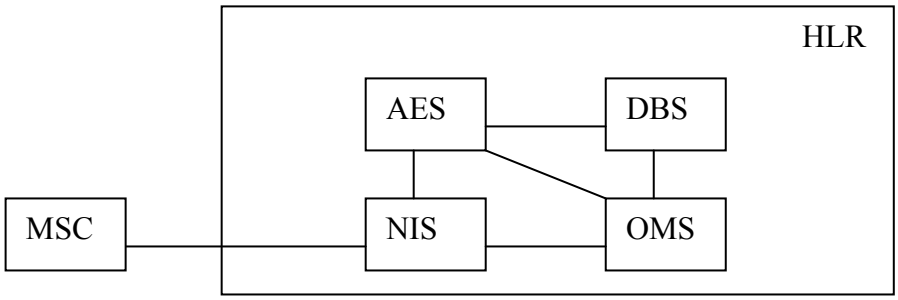
Nhiệm vụ đầu tiên là nhập và xoá thuê bao khỏi mạng. Đăng ký thuê bao cũng có thể rất phức tạp bao gồm nhiều dịch vụ và các tính năng bổ xung. Nhà khai thác phải truy nhập được tất cả các thông số nói trên.

Một nhiệm vụ quan trọng thứ hai của AUC là thực hiện tính cước. Cước phải được tính và gửi đến thuê bao (cố định hay theo yêu cầu tức thời của khách hàng).

Có thể nói rằng mọi tính toán liên quan đến khách hàng đều thực hiện ở AUC, từ tiền cước cho tới các nhiệm vụ tính toán nhận thực. Việc quản lý thuê bao thực hiện thông qua khoá nhận dạng bí mật duy nhất cho từng thuê bao. AUC quản lý các thông tin nhận thực và mật mã liên quan đến từng cá nhân thuê bao dựa trên khoá mật này. AUC có thể được đặt trong HLR hoặc MSC hay độc lập với cả hai. Khoá cũng được lưu trữ vĩnh cửu và bí mật ở bộ nhớ của MS. Tương tự như SIM Card ở GSM, WCDMA cũng sẽ dùng UIM Card để lưu trữ các thông tin này và như vậy có thể rút ra cắm vào được.

- HLR: Home Location Register Bộ đăng ký định vị thường chú

HLR lưu trữ thông tin vĩnh cửu và thông tin tạm thời, như định vị MS, nhận dạng thuê bao, các dịch vụ của MS do nó quản lý, số liệu tính cước, các dịch vụ được phép…. Các số liệu này sẽ được gửi tới mạng khác để nhận thực thuê bao, thông tin dịch vụ hỗ trợ, thông tin cước ….Cấu hình của nó như sau:



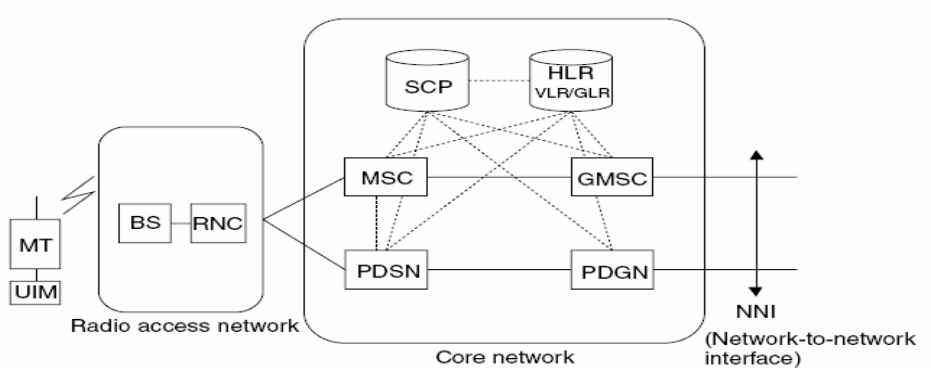
AES	Application Entity Subsystem	Phân hệ ứng dụng
DBS	Database Subsystem	Cơ sở dữ liệu
NIS	Network Interface Subsystem	Phân hệ phối ghép mạng
OMS	Operation & Mainternance Subsystem:	Phân hệ khai thác và bảo dưỡng

Hình 2.9: Cấu hình HLR

Trong mạng lõi còn có:

- GMSC Gateway Mobile Services Switching Center
  Trung tâm chuyển mạch các dịch vụ di động cổng
  Thực hiện kết nối với mạng ngoài thông qua IWF
- MSC Mobile Switching Center: Trung tâm chuyển mạch di động
  Hay còn gọi là MX
- GGSN Gateway GPRS support Note: Điểm hỗ trợ GPRS cổng

Thực hiện kết nối trực tiếp với mạng số công cộng PDN (Public Data Network) phần tử này kế thừa từ mạng GPRS



Hình 2.10 Cấu trúc hệ thống logic WCDMA

❖ *Mạng truy nhập vô tuyến*: chứa các phần tử sau:

- RNC: Radio Network Controller: bộ điều khiển vô tuyến đóng vai trò như BSC ở các mạng thông tin di động
- Nút B đóng vai trò như các BTS ở các mạng thông tin di động
- UE: User Equipment: Thiết bị của người sử dụng

UE bao gồm thiết bị di động ME và mô - đun nhận dạng thuê bao UIM. UIM là vi mạch chứa các thông tin liên quan đến thuê bao (như SIM ở GSM). Giao diện giữa UE và mạng gọi là giao diện Uu. Theo tiêu chuẩn này thì trạm gốc được gọi là nút B. Nút B được nối đến một bộ điều khiển mạng vô tuyến RNC. RNC điều khiển các tài nguyên vô tuyến của các nút B được nối với nó. RNC đóng vai trò như BSC ở GSM (như hình 2.8 ta thấy được sự chuyển tiếp thiết bị giữa hai thế hệ di động khi có sự phối hợp cả GSM và WCDMA).

RNC kết hợp với các nút B nối với nó được gọi là: Hệ thống con mạng vô tuyến RNS (Radio Network Subsystem). Giao diện giữa nút B và RNC được gọi là giao diện Iubis. Khác với giao diện Abis trong GSM ở cùng vị trí (giao diện giữa BSC và BTS) giao diện Iubis được tiêu chuẩn hoá hoàn toàn và để mở, vì thế có thể kết nối nút B của nhà sản xuất này với RNC của nhà sản xuất khác (trong GSM hai thiết bị này được khuyến cáo nên cùng mua một nhà sản xuất). trong mạng truy nhập vô tuyến có cả giao diện giữa các RNC. Giao diện này được gọi là Iur có tác dụng hỗ trợ tính di động giữa các RNC và chuyển giao giữa các nút B nối đến các RNC khác nhau.

Tất cả các giao diện ở mạng truy cập vô tuyến UTRAN đều xây dựng trên cơ sở ATM. ATM được chọn vì nó có khả năng hỗ trợ nhiều loại dịch vụ khác nhau (chẳng hạn tốc độ bit khả biến cho các dịch vụ chuyển mạch gói và có tốc độ không đổi đối với các dịch vụ chuyển mạch kênh). Mặt khác mạng lõi sử dụng cùng kiến trúc cơ sở như kiến trúc của GSM/GPRS, nhờ vậy công nghệ mạng lõi hiện có sẽ có khả năng nâng cấp để hỗ trợ công nghệ truy nhập vô tuyến mới. Chẳng hạn có thể nâng cấp mạng lõi để hỗ trợ UTRAN sao cho một MSC có thể nối đến cả RNC và BSC của GSM.

Trong thực tế các tiêu chuẩn của WCDMA cho phép hỗ trợ chuyển giao cứng giữa WCDMA và GSM và ngược lại. Đây là yêu cầu rất quan trọng vì cần có thời gian để triển khai rộng khắp WCDMA nên sẽ có khoảng trống trong vùng phủ sóng của WCDMA và vì thế thuê bao phải nhận dịch vụ tương ứng tại vùng phủ của GSM.

- ***Các kênh vô tuyến của WCDMA***

Cấu trúc kênh WCDMA được phân thành hai tập kênh: tập kênh theo chiều thuận (hay chiều xuống từ BS (hoặc nút B - do có sự xen kẽ giữa các hệ thống) đến MS (UE)) và tập kênh theo chiều ngược (hay chiều lên từ MS (UE) đến BS (hoặc nút B)) (*)

Các kênh của hệ thống WCDMA thoả mãn các tính chất sau đây:

- Phù hợp với cả ứng dụng tốc độ cao và tốc độ thấp
- Hệ thống có 128 kênh trên mỗi tế bào nếu độ rộng băng tần là 5 Mhz, có 256 kênh nếu độ rộng băng tần là 10 Mhz, hoặc 384 kênh nếu băng tần là 15 Mhz với các cơ chế chống nhiễu cùng kênh phù hợp
- Tiếng nói được mã hoá bằng băng rộng với tốc độ 64 Kbps. Nhưng tốc độ dữ liệu có thể nâng nên thành 144 Kbps tương ứng với tốc độ ISDN, ngoài ra nó còn có thể phục vụ các tốc độ 16 và 32 Kbps

(*) Để thuận tiện cho cách gọi và do có sự tương đương về chức năng, từ đây chúng ta có thể coi BS và nút B là tương đương (thường gọi là BS), tương tự MS và UE là tương đương (thường gọi là MS).

Chương 3: Các mối đe doạ đối với hệ thống và phương pháp bảo vệ

Các mối đe doạ xâm nhập vào hệ thống được chia thành 2 loại: xâm nhập thụ động và xâm nhập tích cực

3.1. *Xâm nhập thụ động*

Xâm nhập thụ động là một hệ thống mưu toan thực hiện vượt qua hàng rào bảo vệ để thu những thông tin dữ liệu trên kênh truyền mà không làm sai lệch nội dung thông tin dữ liệu. Loại xâm nhập này đối với các hệ thống truyền tin đã xuất hiện từ thời phát minh ra điện báo. Trước khi có việc ghép kênh thì việc thu trộm thông tin trên đường truyền tin rất đơn giản. Việc nghe trộm điện thoại trên một đường kết nối cục bộ cũng được thực hiện rất dễ dàng. Ngày nay trong các mạng truyền dữ liệu với các dạng ghép kênh khác nhau và các giao thức phức tạp thì việc thu trộm hoặc phá hoại thông tin dữ liệu trên đường truyền có khó khăn phức tạp hơn, cần có các thiết bị đặc biệt và các chuyên gia kỹ thuật. Nhưng cũng cần lưu ý rằng, các thiết bị đặc biệt đó có thể kiếm rất dễ dàng trên thị trường và các chuyên gia biết kỹ thuật đó cũng không phải là ít.

Trong thông tin vô tuyến loại xâm nhập này là việc thực hiện nghe lén qua đường truyền vô tuyến bằng các bộ thu để xem hai bên bị nghe lén trao đổi với nhau những gì, loại xâm nhập kiểu này ta thấy rất phổ biến trong nghiệp vụ tình báo trong chiến tranh và ngay cả trong thời bình.

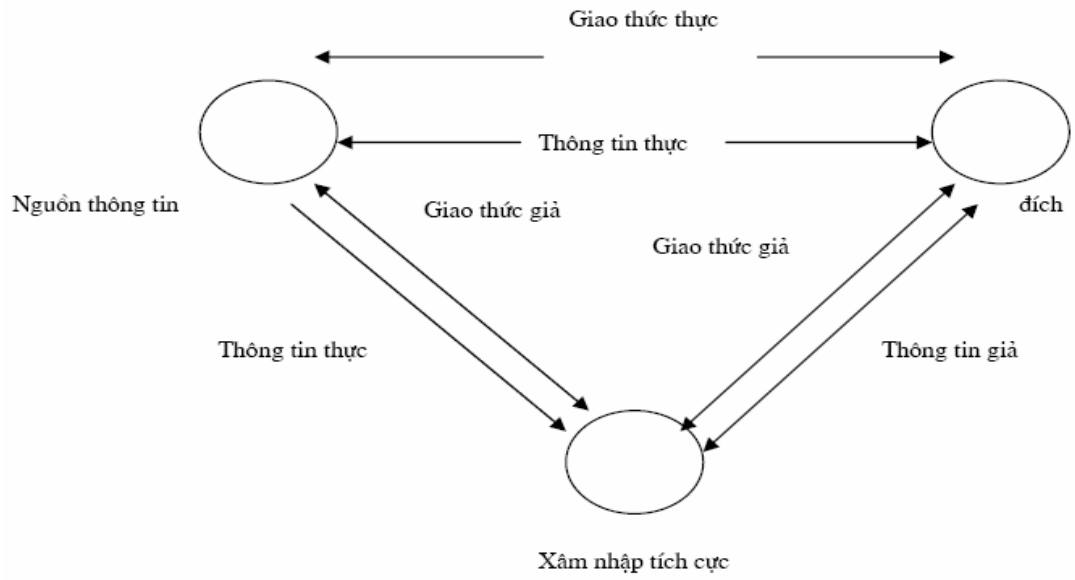
Cũng có ý kiến cho rằng việc ghép kênh phức tạp có thể bảo vệ chống lại các xâm nhập, điều đó là sai lầm và nguy hiểm vì thực ra ghép kênh là sự sắp xếp lại theo một trật tự định sẵn và tuân theo quy định về mặt thời gian, mà đã tuân theo quy luật về mặt thời gian thì kẻ phá hoại dễ dàng định thời thiết bị để có thể thu chính xác các bit dữ liệu cần thiết trên kênh truyền tại các khe thời gian tương ứng.

Một sự rẽ nhánh thụ động không cần thiết phải lọt qua các giao thức kiểm tra dòng dữ liệu. Người ta có thể kiểm tra phát hiện một sự rẽ nhánh thụ động trên đường truyền vật lý bằng cách đo chính xác các đặc tính kỹ thuật của đường truyền. Nhưng việc đo lường các thông số đó không thể thực hiện được trong trường hợp đường truyền kết nối vô tuyến. Để bảo vệ chống lại các xâm nhập thụ động trong các trường hợp này chỉ có cách dùng phương pháp mật mã hoá để bảo vệ dữ liệu truyền.

3.2. *Xâm nhập tích cực*

Các xâm nhập tích cực là mối nguy hiểm tiềm tàng. Ở đây, kẻ xâm nhập tìm cách làm sai lạc các dữ liệu truyền hoặc các dữ liệu lưu trữ và hy vọng rằng, chủ sở hữu hoặc người sử dụng hợp pháp không nhận biết được việc làm này. Việc làm sai lạc các dữ liệu được lưu trữ có thể gây ra do sử dụng sai lạc đường truyền của các đường truy nhập. Ở đây sẽ không đề cập đến các thủ tục truy nhập, mặt dù đó là một chủ đề quan trọng, mà chỉ đề cập đến vấn đề bảo vệ dữ liệu chống lại các xâm nhập bằng các phương pháp ám muội. Trên đường truyền có thể sử dụng các phương pháp mật mã để bảo vệ chống lại các xâm nhập tích cực làm sai lạc dữ liệu. Để thực hiện được điều đó thì cần phải thì cần phải có một cấu trúc mã sao cho tất cả các sự làm sai lệch cấu trúc dữ liệu sẽ không thể thực hiện được nếu không phân tích được mã. Đối với dữ liệu lưu trữ một khi mà kẻ xâm nhập sử dụng phương tiện xâm nhập bất hợp pháp vào một cơ sở dữ liệu thì việc phá hoại các dữ liệu không thể tránh khỏi. Đó là một chủ đề lớn thuộc lĩnh vực bảo vệ dữ liệu lưu trữ. Do đó phải có các biện pháp thích hợp bảo vệ việc xâm nhập bất hợp pháp như: đặt mật khẩu, bức tường lửa…

Một sự xâm nhập tích cực trên đường truyền tin hầu như cũng khó ngăn chặn giống như các xâm nhập thụ động. Tuy vậy việc phát hiện ra chúng thì dễ hơn nhiều. Việc phát hiện sai lạc các dữ liệu có thể được thực hiện được bằng cách đo độ chính xác của thời gian truyền.



Hình 3.1 Mô tả một xâm nhập tích cực

Ở các đường truyền vô tuyến thì rất khó phát giác việc xâm nhập. Đây thực sự là một cuộc đấu trí căng thẳng giữa một bên cố gắng bảo toàn sự trọn vẹn và bảo mật

dữ liệu của mình và cố nhận ra những xâm nhập bất hợp pháp, còn một bên không kém phần tài năng là kẻ xâm nhập, người mà bằng mọi cách lấy cho bằng được thông tin từ bên phát, bằng mọi cách che đậy hành động của mình vì có như vậy thì bên bị xâm nhập không biết được đang bị phá hoại, để có thể đạt được mục đích của mình hoặc tiếp tục khai thác những lần sau. Nếu như một đường vật lý được giám sát chặt chẽ và thường xuyên, lưu lượng truyền được kiểm tra thường xuyên thì lúc đó hầu như không một sự xâm nhập nào không được phát hiện.

Việc thực hiện một xâm nhập rẽ nhánh tích cực là một công việc không đơn giản. Ở hình 3.1 việc truyền việc truyền tin giữa nguồn và đầu cuối được điều khiển bởi một giao thức được gọi là "giao thức thực". Việc xâm nhập tích cực phải ngắt giao thức đó và đưa vào một "giao thức giả". Như vậy các thông tin thực sẽ từ nguồn về kẻ xâm nhập và thông tin giả từ kẻ xâm nhập về đầu cuối mà đầu cuối không nhận biết được. Với một số biến đổi, việc xâm nhập tích cực như trên có thể thiết lập được với kênh truyền tin. Nếu mạng truyền tin là mạng diện rộng, mạng vô tuyến đã chuẩn hoá, hoặc nối mạng Internet thì việc thiết lập xâm nhập tích cực trên càng có điều kiện, bởi vì các giao thức truyền tin đã được công bố.

3.3. *Các phương pháp bảo vệ*

Việc bảo vệ các dữ liệu truyền chống lại các xâm nhập tích cực cũng dựa trên các nguyên lý giống như bảo vệ các dữ liệu lưu trữ. Nó có thể ngăn ngừa việc làm sai lạc, thêm vào, phá hoại dữ liệu hoặc việc các dữ liệu bị làm lặp lại (thu rồi phát lại nhiều lần bởi kẻ xâm nhập). Trong các khối dữ liệu truyền thì việc làm sai lạc, việc thêm vào hoặc phá hoại dữ liệu sẽ liên quan đến tất cả các khối dữ liệu được mã hoá, có nghĩa là toàn bộ khối dữ liệu mã hoá phụ thuộc vào khối dữ liệu rõ tương ứng cũng như cả khối dữ liệu rõ trước nó. Một sự xâm nhập sẽ không thể thực hiện được nếu không tìm được khoá mã theo kiểu thám mã.

Vấn đề kẻ xâm nhập thực hiện việc phát lặp lại là dạng xâm nhập mà kẻ thực hiện việc phá hoại bằng cách đơn giản là ghi lại các dữ liệu mã hoá đã được truyền để rồi sau đó thực hiện phát lại bản tin này đến nơi cần nhận, thậm chí bản thân kẻ xâm nhập cũng chẳng hề biết bản tin đó nội dung như thế nào. Vấn đề này đặc biệt nghiêm trọng trong công việc ngân hàng, tài chính, vì một tài khoản của đối tác có thể được truyền đến nơi nhận nhiều lần làm cho số tài khoản của đối tác thay đổi ngoài mong muốn. Có thể ngăn ngừa vấn đề này bằng cách kết hợp đánh số bản tin phát (mỗi bản tin sẽ đính kèm với một số thứ tự), và nhận dạng bên phát.

3.4. *Các phép mật mã hoá bảo vệ khỏi các xâm nhập thụ động*

Như thảo luận ở trên chúng ta cần phải bảo vệ dữ liệu khỏi các xâm nhập thụ động và phương pháp hiệu quả nhất là thực hiện mật mã hoá. Vậy việc mật mã hoá là gì? Việc mật mã hoá là quá trình chuyển thông tin có thể gọi là *bản tin rõ* thành thông tin không thể đọc được theo cách thông thường gọi là *bản mã*. Việc giải mật mã là quá trình ngược lại, giải mã là quá trình chuyển thông tin ngược lại từ *bản mã* thành *bản tin rõ*. Các phương pháp mật mã hoá bao gồm các loại như mã dòng là mật mã hoá theo kiểu thay thế một ký tự bằng một ký tự khác, và mã khối là phương pháp mật mã thực hiện biến đổi cả khối bản tin rõ thành một khối mã (khối bit)...

Nếu ký hiệu hệ mã hoá là bộ (P, C, K, e, d)

P: Tập hữu hạn các bản rõ

C: Tập hữu hạn các bản mã

K: Tập hữu hạn các khoá (không gian khoá)

e: Hàm mã hoá P -> C

d: Hàm giải mã C -> P

Có thể liệt kê một số phương pháp mật mã hoá như sau:

- Hệ mã dịch chuyển

  Hệ mã dịch chuyển là bộ (P, C, K, e, d) với:

  P: Z_{26}

  C: Z_{26}

  K: Z_{26}

0	1	2	3	4	5 ….	23	24	25
A	B	C	D	E	F	X	Y	Z

  e: X -> Y = (X +k) mod 26

  d: Y -> X = (Y - k) mod 26

  Ví dụ: với k = 4;

  1. Nhập bản tin rõ chữ RC = CHIEUNAYLOGACH
  2. rõ chữ -> rõ số RS = 2| 7| 8| 4| 20| 13| 0| 24| 11| 14| 6| 0| 2| 7
  3. rõ số -> mã số MS = 6| 11| 12| 8| 24| 17| 4| 2| 15| 18| 10| 4| 6| 11

4. mã số -> mã chữ: MC = GLMIYRECPSKEGL

Độ an toàn 25 giá trị (thực ra chỉ cần 24)

- Hệ mã thay thế

Là phương pháp thay thế bản tin rõ bằng các chữ cái tương ứng nhưng với một bảng chữ cái sắp xếp "không theo trật tự", Sự thế phụ thuộc vào bản thân chữ cái được thay thế.

Trong đó P: Z_{26} ; C: Z_{26} ; K: Z_{26}

RC = CHIEUNAYLOGACH

MC = QMNRGUHJIFOHQM

Độ an toàn 26! (khoảng 4.10^{26}) rõ dàng được cải thiện đáng kể so với phương pháp mã dịch chuyển.

- Hệ mã Affine

Là bộ (P, C, K, e, d): P: Z_{26} ; C: Z_{26} ; K: Z_{26}

K = (a, b) trong đó a: nguyên tố cùng nhau với 26 hay UCLN (a, 26) = 1, và b $\in Z_{26}$

a^{-1} phần tử nghịch đảo của a theo Mod 26 hay a * a^{-1} = 1 Mod 26

e: X -> Y = (a * X + b) Mod 26 và d: Y-> X = a^{-1} * (Y-b) Mod 26

Ví dụ:

RC = CHIEUNAYVUONHOA

RS = 2| 7| …

MS = 12| 1| 4|…

Chọn (a, b) = (3, 6)

(3*2 + 6) Mod 26 = 12

(7*2 +6) Mod 26 = 1….

Ngoài ra còn có các phương pháp khác như:

- Hệ hoán vị cục bộ

Trong đó bản tin rõ sẽ được chia thành các đoạn nhỏ hơn, và thay thế ký tự bằng các quy luật khác nhau

- Hệ mã hóa Vigenere

Trong đó dùng một bộ khoá k hoán vị theo một ma trận k cho sẵn với mỗi lần nhận một giá trị k khác nhau trong m chìa khoá, m tuỳ ý

$k = k_1, k_2, k_3 \ldots k_m$

- Hệ mã hoá Hill

Với dùng bộ khoá k là một ma trận với quy luật lấy khoá k khác nhau

….

Nhận xét: Ta thấy rằng ở đây tất cả các phương pháp mật mã hoá là nhằm cho kẻ xâm nhập không còn thấy gì hết, đọc được bản tin đã mã như nhìn một "mớ hỗn độn" chữ linh tinh, nếu như kỹ thuật mật mã càng cao thì khả năng thám mã để đọc được bản tin rõ ban đầu càng lâu và thuật toán đó càng có tính bảo mật cao

3.5. *Sự xâm nhập vào các dữ liệu được mã hoá để giải mã*

Trước khi vai trò của máy tính nên ngôi thì việc mã hoá và giải mã các bản tin mật chủ yếu dựa vào tài năng khôn khéo của con người và nó có thể là một bí quyết nào đó. Với tất cả các loại mã cổ điển thì việc phân tích một bản tin đã mã hoá đều có thể thực hiện được bằng cách này hay cách khác. Sự ra đời của máy tính đã giúp cho công việc mã hoá và giải mã tiến một bước khá dài. Máy tính có thể thực hiện các phép tính phức tạp trong một thời gian ngắn mà bằng các phương pháp khác phải mất hàng năm hoặc hàng chục năm mới thực hiện được.

Một người nào đó nhận được bản tin vô tuyến mà nội dung đoạn tin được mã hoá sẽ gặp phải vấn đề: hệ thống điều chế có thể phức tạp, ngôn ngữ của bản tin rõ chưa biết và phương thức mã hoá khoá mã cũng chưa biết.Thông thường trong trường hợp này người đó phải thử áp dụng tất cả các phương thức mà mình đã biết và các khoá mã cho là có khả năng nhất, tất nhiên là thời gian tính toán mỗi phương án phải đủ nhỏ, nhưng nói chung để tìm ra phương thức đúng thì hầu như là phải thử tất cả các khả năng theo cách thám mã. Đoạn tin đó dù có rất quan trọng nhưng người đó không thể nhận biết được nếu như công sức để khám phá ra đoạn tin đó vượt qua giới hạn cho phép (chủ yếu về mặt thời gian).

Nói cho công bằng thì không có một phương pháp mã nào là không bị phá nhưng thời gian để thực hiện thám mã trong không gian khoá (như khoá k ở các thuật toán đã giới thiệu trên chẳng hạn) sẽ là vấn đề mấu chốt của thuật toán mật mã hoá mà kẻ xâm nhập phải đương đầu, và tất nhiên với người truyền tin thời gian này càng lâu càng tốt. Việc đánh giá độ mật của một phép mật mã thường được giả thiết rằng, thuật

toán mã đã biết và vấn đề còn lại là giải mã đoạn tin đã nhận được bằng cách khám phá ra khoá mã. Công việc sẽ là khó khăn cho người phân tích mã bởi duy nhất chỉ dựa vào bản tin đã được mã hoá, không có thông tin gì về bản tin rõ. Nếu như không có một sự dư thừa nào trong bản tin, thì việc khám phá ra mã sẽ gặp nhiều khó khăn. Nếu như biết được một phần nào đó của bản tin rõ thì bài toán có thể trở nên đơn giản hơn rất nhiều, ví dụ trong bản tin có phần tiêu đề được viết theo chuẩn là một trong những nơi có thể khai thác đầu tiên. Các khoá có thể được thử lần lượt cho đến khi phần tiêu đề được thừa nhận xuất hiện trong bản tin được giải mã. Nếu phần tiêu đề theo chuẩn đó càng dài thì việc nhận dạng khoá càng chính xác. Nếu tiêu đề ngắn thì có thể tập hợp nhiều bản được giải mã để lựa chọn các khoá có khả năng. Việc biết mã hoá sử dụng cho bản tin rõ, bao gồm ví dụ như bit kiểm tra chẵn lẻ cũng là một yếu tố có lợi cho người phân tích mã. Cũng vì vậy mà trong nhiều trường hợp khoá mã không sử dụng bit kiểm tra chẵn lẻ.

Nếu người phân tích mã không những chỉ có bản tin đã mã hoá, mà có bản tin rõ tương ứng thì việc khám phá khoá mã sẽ gặp nhiều thuận lợi. Công việc ở đây chỉ còn là khám phá khoá mã cho bản tin rõ và bản tin đã mã hoá. Nếu chiều dài bản tin đủ lớn, thì khoá mã có thể nhận dạng được với độ chính xác tuyệt đối.

Khi muốn tin chắc vào độ bảo mật của mật mã đã thực hiện thì thường đặt giả thiết là kẻ xâm nhập có những yếu tố thuận lợi nhất để khám phá. Cụ thể là, kẻ xâm nhập có thể được biết thuật toán thực hiện và chúng có thể có một số lượng khá đủ các bản tin rõ và bản mã đã được mã hoá tương ứng. Điều này là khả năng xấu nhất nhưng hoàn toàn có thể trong thực tế. Có thể hình dung ra rằng, một kẻ xâm nhập có thể, ví dụ như chèn một đoạn tin riêng vào trong đường truyền, và sau đó bằng cách này hay cách khác, có thể thu lại được bản tin rõ tương ứng. Cũng chính vì vậy mà một mật mã tốt nhất phải tính đến hết tất cả các khả năng xâm nhập.

Vậy mật mã được sử dụng trước hết là để bảo đảm tính bí mật cho các thông tin được trao đổi, và do đó bài toán quan trọng nhất của thám mã cũng là bài toán phá bỏ tính bí mật đó, tức là từ bản mật mã có thể thu được dễ dàng trên kênh vô tuyến hoặc trên kênh truyền dẫn công cộng, người thám mã phải phát hiện được nội dung thông tin được che dấu trong bản tin mật mã đó, mà tốt nhất là tìm ra được bản tin gốc của bản mật mã đó, Tình huống thường gặp là bản thân sơ đồ hệ thống mật mã, kể cả các phép lập mã và giải mã, không nhất thiết phải bí mật, do đó bài toán quy về việc *tìm chìa khoá mật mã k,* hay chìa khoá giải mã k’ nếu như hệ mật mã đó có khoá phi đối xứng (là hệ khoá biết được khoá mã hoá cũng rất khó khăn tìm được khoá giải mã - hệ thống có khoá mã công khai). Ngoài các thông tin về sơ đồ mã hoá và giải mã người

thám mã còn có thể biết các thông tin khác và dựa vào các thông tin biết được ta chia thành các bài toán thám mã như sau:

- Bài toán thám mã chỉ biết *bản mã*: là bài toán phổ biến nhất, khi đó người thám mã chỉ biết một bản mật mã Y
- Bài toán thám mã biết cả *bản mã và bản rõ*: người thám mã biết một bản tin mật mã Y cùng với bản tin rõ tương ứng X
- Bài toán thám mã khi có *bản tin rõ được chọn*: người thám mã có thể chọn một bản tin rõ X, và biết bản mật tương ứng Y. Điều này xảy ra khi người thám mã chiếm được (tạm thời) máy lập mã
- Bài toán thám mã khi có *bản tin mã được chọn*: người thám mã có thể chọn bản mật mã Y, và biết được bản tin rõ tương ứng. Điều này có thể xảy ra khi người thám mã chiếm được tạm thời máy giải mã.

Nếu như kẻ xâm nhập thực hiện một công việc tìm kiếm tất cả các khoá mã có thể sử dụng trong một máy tính theo phương pháp cặp "bản tin rõ – bản tin đã mã hoá" thì chúng ta có thể đánh giá thời gian cần thiết để thực hiện giải mã xuất phát từ thời gian cần thiết để tìm khoá mã tương ứng với chiều dài của khóa và tốc độ thử cho phép

Chiều dài khoá mã (bit)	phép thử đơn giản		10^6 phép thử song song	
	10^{-3} s	10^{-6} s	10^{-3} s	10^{-6} s
24	2.33 h	8.4 s	8.4 ms	8.4"s
32	24.9 d	35.8 d	2.15 s	2.15 ms
40	17.4 y	6.4 m	9.2 d	550 ms
48	>100 y	4.64 y	1.64 m	2.45 h
56		> 100 y	1.14 y	10.0 d
64			> 100 y	107 d

Bảng 3.2 Mô tả cùng khoá tốt (được đánh dấu đậm) có thể sử dụng

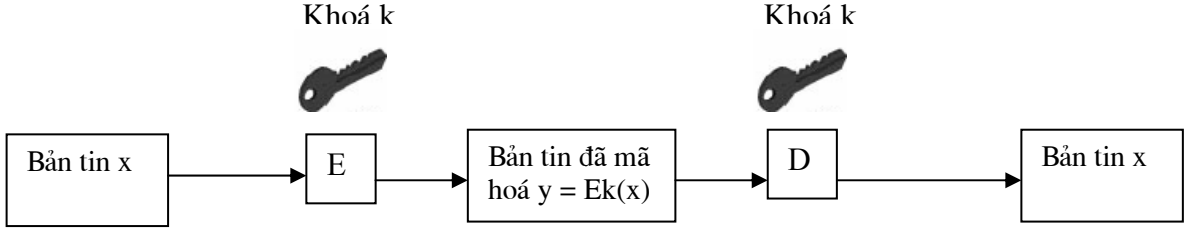
Trong đó: d = ngày, m = tháng, y = năm

Như vậy đối với hệ thống thông tin vô tuyến với khả năng tính toán của máy tính hiện nay càng cao, ta cần phải có những biện pháp mạnh để chống lại cách thám mã này một trong đó là đơn giản tăng chiều dài của khoá mã. Trong công nghệ WCDMA việc mật mã hoá thông tin trên đường cũng dựa theo nguyên lý này với khoá có chiều dài đủ lớn.

Chương 4: Một số thuật toán cơ sở được áp dụng

Trong tất cả các phương pháp bảo mật thì phương pháp sử dụng khoá mã có tính an toàn cao nhất, các thuật toán mã hoá không dùng khoá mã rất dễ phán đoán. Trong các thuật toán mã hoá có sử dụng khoá mã thì quá trình mã hoá được thực hiện dưới sự điều khiển của khoá mã, nó làm gia tăng sự hoàn thiện của thuật toán. Thực tế là không phải bản thân phép mã hoá, mà chính độ phức tạp của khoá mã sẽ quyết định rằng việc mã hoá có đạt hiệu quả mong muốn hay không và thời gian an toàn của phép mã hoá, tức là độ bảo mật của phép mã hoá khi có kẻ nào đó cố gắng phá khoá, là dài hay ngắn. Như vậy độ mật của mật mã không phải ở thuật toán mà ở khoá mã, mọi thuật toán đối phương đều có thể có vì khi đã thành chuẩn rồi thì mọi người đều có thể biết. Chính vì vậy mà trách nhiệm của người quản lý hệ thống là thực hiện tạo khoá, phân phối khoá, sử dụng khoá và huỷ khoá sau khi sử dụng một cách hiệu quả nhất.

Mục đích của việc mã hoá là che dấu thông tin trước khi truyền trên kênh. Chúng ta mô hình hoá phép mã hoá và giải mã như sau:



Hình 4.1. Mô hình hoá phép mã hoá và giải mã.

Các ký tự E và D là các ký hiệu cho các hàm giải mã và mã hoá, biểu thức toán học của phép mã hoá là:

$$y = Ek(x)$$

Và phép giải mã là:

$$x = Dk(y)$$

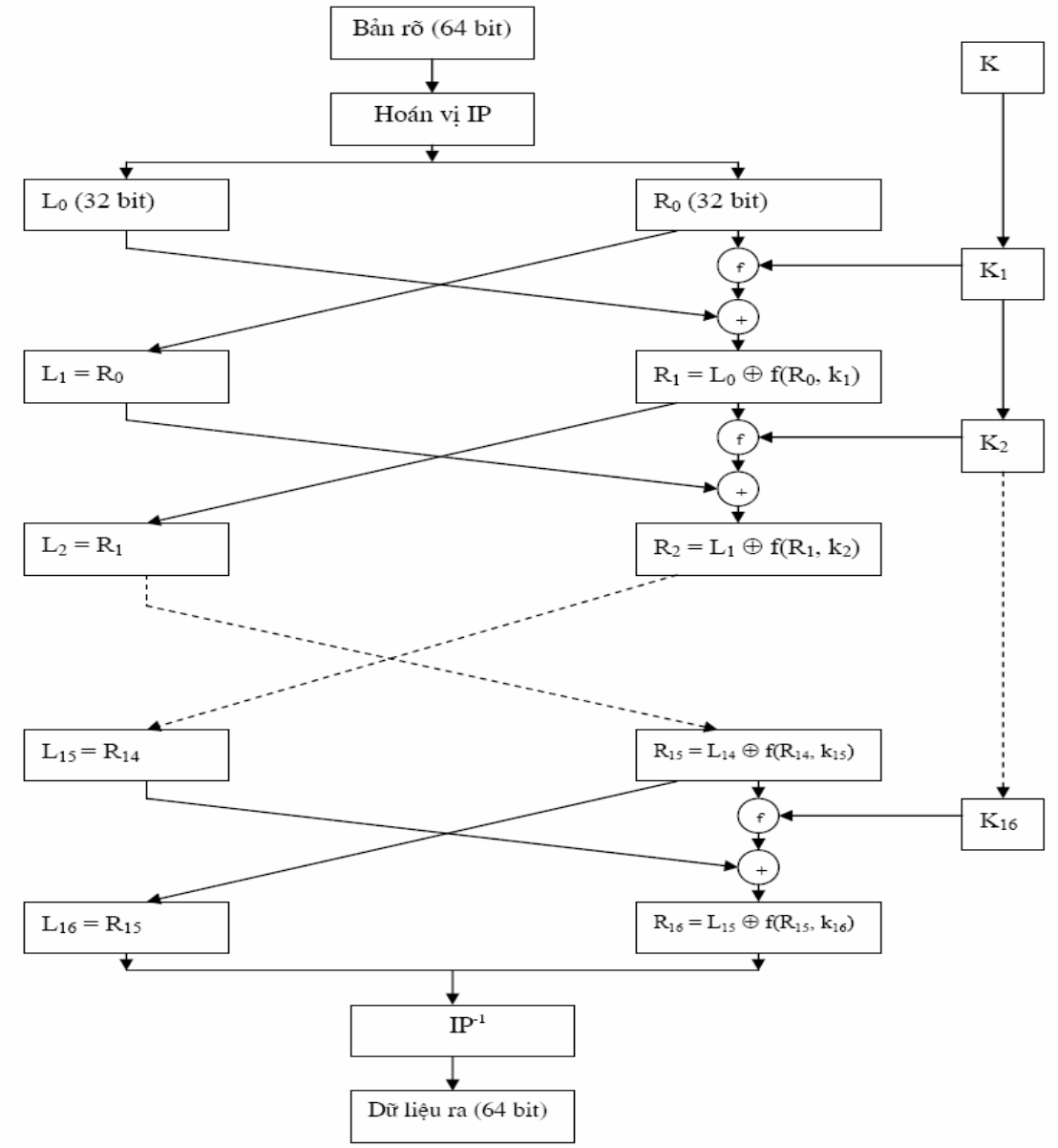
Trong đó tham số phụ k là khoá mã

Sau đây chúng ta xem xét một số thuật toán làm cơ sở toán học cho thuật toán nhận thực.

4.1. *Thuật toán DES*

Vào những năm 70, hãng IBM đề xuất thuật toán Lucifer. Thuật toán đó đáp ứng được các yêu cầu của cơ quan chuẩn quốc gia Mỹ NBS (National Bureau of Standard)

và được ứng dụng ở các ngân hàng tự động. Sau đó nó được phát triển thành thuật toán mã chuẩn DES và được đưa ra dùng cho các ứng dụng chung và được gọi là chuẩn mã bảo mật dữ liệu DES (Data Encryption Standard). Thuật toán DES là một giải thuật mật mã đối xứng đang được ứng dụng rộng rãi và còn có tên gọi là thuật toán mật mã dữ liệu DEA (Data Encryption Algorithm). Sơ đồ thực hiện như sau:



Hình 4.2: sơ đồ thực hiện thuật toán DES

Các phần tử cấu thành của thuật toán là các phép thay thế, chuyển vị và phép cộng module 2.

Phép chuyển vị trong DES có 3 dạng:

- Chuyển vị bình thường: số bit đầu ra bằng số bit đầu vào.

- Chuyển vị lựa chọn: số bit đầu ra nhỏ hơn số bit đầu vào.
- Chuyển vị mở rộng: số bit đầu ra lớn hơn số bit đầu vào, các bit có thể lặp lại.

➢ ***Các bước thực hiện***

1. 64 bit của 8 byte ban đầu được cho vào chuyển vị thành 64 bit đầu ra theo phép chuyển vị khởi đầu IP (Initial Permutation) thực hiện bằng phép chuyển vị thông thường tạo ra 8 khối mỗi khối 8 bit theo bảng sau:

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Hình 4.3 Sắp xếp các bit dữ liệu trong chuyển vị khởi đầu IP của thuật toán DES

Tương ứng như trên ta thấy bit ra thứ nhất chính là bit thứ 58 của 64 bit đầu vào, bit ra thứ hai tương ứng với bit thứ 50 của khối 64 bit đầu vào…

2. 64 bit đầu ra được chia thành 2 phân khối, mỗi phân khối 32 bit gọi là phân khối trái L và phân khối phải R cho vào 2 thanh ghi riêng biệt để thực hiện biến đổi tiếp, thanh ghi R được đưa vào chuyển vị bằng phép chuyển vị mở rộng, 32 bit đầu vào thành 48 bit đầu ra, tuân theo bảng sau:

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Hình 4.4: Bảng chuyển vị có mở rộng E của thuật toán DES

3. 48 bit đầu ra của phép chuyển vị mở rộng được cộng module-2 với các bit xuất phát từ khoá mã, sau đó chia thành 8 hộp S, mỗi hộp 6 bit, các hộp này đưa vào chuyển vị một lần nữa bằng phép chuyển vị lựa chọn mà theo đó 6 bit đầu vào sẽ cho ra 4 bit đầu ra (theo cách này 2 bit đầu tiên và cuối cùng để tham chiếu dòng và 4 bit giữa để tham chiếu cột của bảng), theo bảng sau:

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	6	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	8	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	1	11	6
4	3	2	12	9	5	15	10	11	14	11	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Hình 4.5. Bảng mô tả các biến đổi các hộp S của thuật toán DES

4. 32 bit từ 8 hộp S được nhóm lại với nhau và đưa vào bộ chuyển vị P theo bảng sau đây

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Hình 4.6: Bảng chuyển vị P của thuật toán DES

32 bit đầu ra của bộ chuyển vị P được cộng module -2 với 32 bit khởi đầu của thanh ghi L và kết quả được đặt vào thanh ghi R, để phép thực hiện này không bị sai lệch một thanh ghi đệm 32 bit được đặt vào giữa thanh ghi R và bộ cộng Module-2.

Chu trình trên được lặp lại 16 lần, sau đó nội dung của các thanh ghi R và L được tập hợp trong một khối 64 bit theo trật tự R trước L sau. Cuối cùng khối này sau đó sẽ được chuyển vị nghịch đảo của chuyển vị ban đầu IP^{-1} theo ma trận sau, ta sẽ thu được kết quả cuối cùng của thuật toán có độ dài 64 bit:

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Hình 4.7. Bảng chuyển vị IP^{-1}

Mỗi lần thực hiện một chu trình chính đó gọi là "một vòng".

Các khoá mã đã tham gia vào quá trình trên như thế nào? Câu trả lời đã có trong phần trên, đầu ra của chuyển vị có mở rộng E là 48 bit dữ liệu và 48 bit dữ liệu đó được cộng Module-2 với 48 bit mã khoá (và như vậy không gian mã hoá sẽ là 2^{48}). Với mỗi chu trình thì các bit khoá sẽ có các giá trị khác nhau.

- ***Thực hiện tạo khoá***

64 bit tạo khoá mã được đưa vào thanh ghi khoá mã sau đó được đưa vào bộ chuyển vị PC1 (bộ chuyển vị lựa chọn một), theo ma trận sau:

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Hình 4.8 Bảng chuyển vị PC1

Đầu ra của bộ chuyển vị PC1 được đặt trong hai thanh ghi C và D. Khoá mã 56 bit đó cũng được phân làm 2 từ, mỗi từ 28 bit và được đặt trong các thanh ghi C và D. Các thanh ghi C và D là các thanh ghi dịch chuyển vòng: cứ mỗi vòng chu kỳ mã nó chuyển dịch và phía trái một hoặc hai vị trí như mô tả ở hình sau:

Số vòng	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Số bit dịch trái	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Hình 4.9. Bảng dịch chuyển trái của khoá mã (trước PC2)

Nội dung của các thanh ghi C và D được đưa tiếp vào bộ chuyển dịch PC2 để có được 48 bit đầu ra, nó sẽ biến 56 bit đầu vào thành 48 bit cần dùng. Cứ mỗi vòng khác nhau của thuật toán thì đầu ra của chuyển vị PC2 lại cung cấp một khoá mã khác nhau để sử dụng cho chu trình.

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Hình 4.10. Bảng ma trận lựa chọn PC2

Đến thời điểm này việc mã hoá DES đã hoàn thành. Việc giải mã được thực hiện tương tự với việc mã hoá, chỉ có sự khác biệt duy nhất ở phần tạo ra các khoá mã riêng biệt. Ở phần mã hoá, các thanh ghi dịch chuyển vòng về bên trái, trong lúc ở mã hoá chúng dịch chuyển về bên phải với một quy tắc tuân theo bảng tương tự như bảng ở hình dưới đây:

Vòng	Khối khoá	Số chuyển dịch phải (trước PC2)
1	K1	0
2	K2	1
3	K3	2
4	K4	2
5	K5	2
6	K6	2
7	K7	2
8	K8	2
9	K9	1
10	K10	2
11	K11	2
12	K12	2
13	K13	2
14	K14	2
15	K15	2
16	K16	1

Hình 4.11. Bảng dịch chuyển phải của khoá mã khi giải mã

Cấu trúc của bài toán mã hoá ở đây là hoàn toàn đối xứng với giải mã, do vậy thuật toán DES thuộc loại mã đối xứng.

➢ ***Đánh giá hiệu quả của thuật toán DES:***

Kết quả được đánh giá dựa trên bảng thiết lập thay đổi một bit của dãy đầu vào và xem xét sự khác nhau của đầu ra, sau đó tính khoảng cách Hamming giữa các khối tin đã mã hoá và kết quả của chúng ta thu được khoảng cách Hamming thu được là 31.06, một giá trị gần với giá trị mong muốn, theo lý thuyết là 32.

Sau khi thử nghiệm có thể nhận thấy là sau chỉ khoảng 5 chu trình thì đã có rất ít sự tương quan giữa các đầu vào và các kết quả trung gian. Như vậy ta có thể kết luận là với 5 chu trình cũng khá đủ để khắc phục tính điều hoà của hàm số. Thuật toán DES chọn tới 16 chu trình thực hiện được xem như là đã quá đủ để khắc phục tính điều hoà của hàm số.

Chúng ta dễ nhận thấy là độ tin cậy của thuật toán phụ thuộc vào độ dài của của khoá mã (hay không gian khoá mã).

Tuy nhiên thuật toán DES cũng không thể tránh khỏi hạn chế, một trong các hạn chế đó là đặc tính bù của thuật toán, điều này có nghĩa là:

Nếu $y = Ek(x)$ thì $y^{-1} = Ek^{-1}(x^{-1})$.

Nếu biết được kết quả của y và y^{-1} và biết được x cùng với x^{-1} thì việc thám mã sẽ dễ dàng hơn nhiều cho kẻ xâm nhập, tuy nhiên có thể hạn chế điều này bằng cách tăng không gian khoá lên, và hiện nay đã có các thuật toán mới dựa trên thuật toán DES để khắc phục hạn chế này.

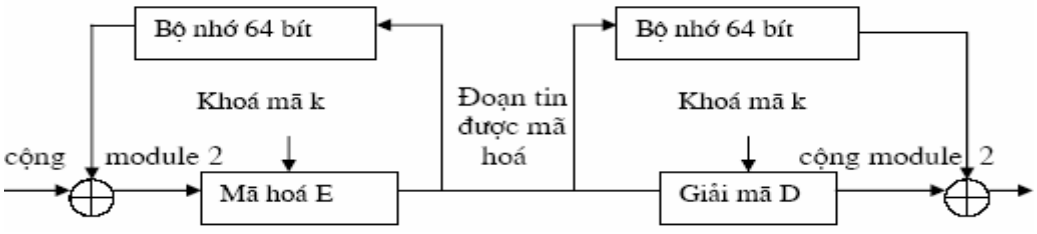
Mật mã khối DES có thể ứng dụng để xử lý các khối dữ liệu có độ dài cố định (thường có độ dài 64 bit) và độ dài của bản tin có thể bất kỳ.

Một trong các kỹ thuật nhận thực trong WCDMA đã áp dụng thuật toán DES trong quá trình tính toán như sẽ được thấy trong chương tiếp theo.

Sau đây chúng ta xem xét một số thuật toán mật mã dựa trên cơ sở thuật toán DES:

4.1.1. Mật mã CBC (Cipher Block Chaining)

Phương pháp này sử dụng đầu ra của phép toán mã hoá để biến đổi đầu vào tiếp theo (nhờ có bộ nhớ đệm). Như vậy, mỗi khối được mã hoá không những chỉ phụ thuộc vào đoạn tương ứng mà còn phụ thuộc vào tất cả các khối được mã hoá của đoạn tin rõ trước nó. Thuật toán được thực hiện như lược đồ dưới đây:



Hình 4.12: Sơ đồ khối chức năng của phương pháp mật mã CBC

Trừ khối đầu tiên, tất cả các khối sau đó đều được cộng Module-2 với khối đã được mã hoá trước đó, tức là khối thứ n được mã hoá thành C_n phụ thuộc vào tất cả các khối dữ liệu rõ P_1, P_2, P_3 …,P_{n-1}, P_n. Ở bên nhận quá trình sẽ xảy ra ngược lại, ở đây sau khi giải mã sẽ thực hiện phép cộng Module -2 với khối đã được mã hoá sau nó để được dữ liệu rõ ban đầu. Trong quá trình thực hiện 1 bit của khối dữ liệu vào, P_n được cộng Module-2 với một bit tương ứng của khối dữ liệu đã được mã hoá trước đó C_{n-1}. Các phép toán có thể thực hiện nối tiếp hoặc song song từng byte một. Nếu thực hiện với mật mã DES thì tốc độ của chúng phù hợp với tốc độ của mã DES.

Ta có thể giải thích phương pháp mật mã CBC như sau:

- Với phép mã hoá:

$$C_n = Ek\ (P_n \oplus C_{n-1})$$

- Với phép giải mã:

$$Q_n = Dk\ (C_n) \oplus C_{n-1}$$

Để chứng minh rằng, sẽ xác định được đoạn tin rõ sau khi giải mã, ở đây sẽ dùng phép toán Dk cho biểu thức đầu tiên, ta có:

$$Dk\ (C_n) = P_n \oplus C_{n-1}$$

Thay thế giá trị đó vào biểu thức thứ hai ta sẽ được:

$$Q_n = P_n \oplus C_{n-1} \oplus C_{n-1} = P_n.$$

Việc chọn giá trị khởi đầu cũng rất quan trọng để bảo đảm bí mật ở hai đầu nút (để mà từ đó bảo đảm bí mật cho những dữ liệu sau vì muốn biết được các dữ liệu sau nó thì phải biết được các bit dữ liệu ban đầu do chúng có liên quan đến nhau). Trong trường hợp dùng mật mã CBC cho hệ thống truyền tin thì các giá trị ban đầu đó cần phải giữ hoàn toàn bí mật. Ta thường ký hiệu các giá trị khởi đầu là IV.

Nếu chia thành các đoạn không chẵn ta có thể có hai cách giải quyết đối với đoạn cuối cùng: xử lý đặc biệt và thêm các bit ngẫu nhiên vào để đủ 64 bit.

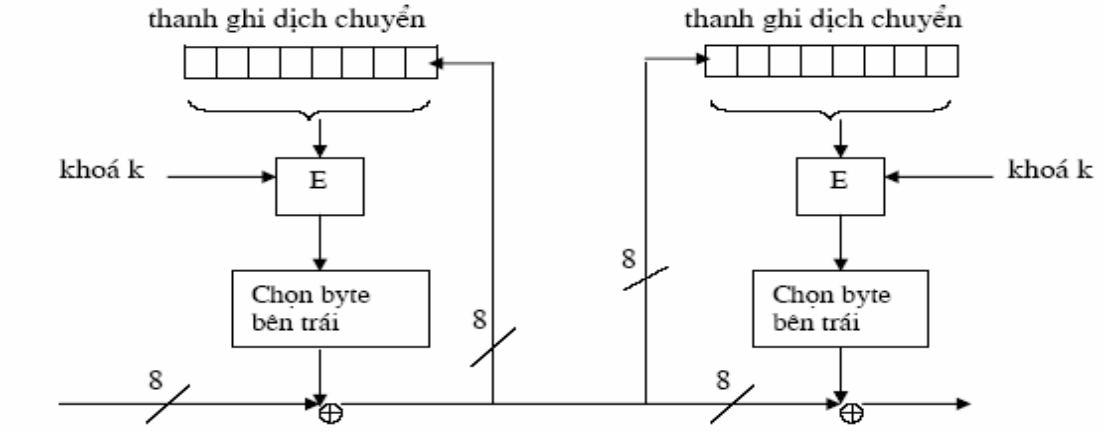
Mật mã CBC được xây dựng trên cơ sở các khối dữ liệu có quan hệ móc xích với nhau, nhằm khắc phục nhược điểm của phương pháp ECB. Điều này chỉ đúng với các khối bắt đầu từ khối thứ hai, còn khối dữ liệu đầu tiên lại phụ thuộc vào các giá trị khởi đầu. Nếu như giá trị khởi đầu luôn là hằng số với tất cả các bản tin thì điều đó tạo tính quy luật cho đối phương dễ phát hiện. Trong thực tế truyền tin các giá trị khởi đầu luôn được thay đổi và người ta cũng tránh việc dùng cùng giá trị khởi đầu và cùng khóa mã nhiều lần cho các bản tin được truyền.

4.1.2. Mật mã CFB (Cipher FeedBack)

Khi phải xử lý các đoạn tin theo byte hoặc theo bit, người ta thường sử dụng một phương pháp mật mã dưới dạng phản hồi đoạn tin đã mã hoá, được gọi là mật mã CFB (Cipher FeedBack). Nguyên lý hoạt động của CFB như hình dưới đây. Nhìn cũng tương tự với phép mã hoá và giải mã của CBC, nhưng khác nhau ở chỗ CFB đã dùng phép mã hóa khối DES trong khối phản hồi đầu vào bên phát và khối phản hồi đầu ra bên thu. Cấu trúc của hệ thống đảm bảo rằng dữ liệu được bổ sung thêm là hoàn toàn giả ngẫu nhiên.

Trong khi phương pháp mật mã CBC thực hiện trên các khối dữ liệu hoàn chỉnh thì phương pháp mật mã CFB thực hiện mỗi lần một chuỗi các bit có độ dài m lựa chọn được. Chiều dài m theo lý thuyết có thể là từ 1 → 64, theo đó chiều dài nhỏ nhất là 1 ứng với trường hợp mật mã CFC một bit. Hiện nay trên các hệ thống truyền tin phổ biến nhất là sử dụng m = 8 (mã hoá theo byte).

Cũng giống như mật mã CBC, phương pháp mật mã CFB liên kết các ký tự với nhau và làm cho bản tin được mã hoá vào toàn bộ bản tin rõ.



Hình 4.13: Sơ đồ nguyên lý hoạt động của việc mã hoá và giải mã CFB

Trong đó E là khối mã hoá theo thuật toán DES

Giống như CBC, Phương pháp mật mã CFB cũng cần có một giá trị khởi đầu. Ta cũng sẽ sử dụng các giá trị khởi đầu khác nhau để tránh đặc tính chu kỳ. Điều đáng chú ý là các giá trị khởi đầu có thể truyền công khai bởi vì chúng đã trải qua phép toán mã hoá, vì thế rất thuận lợi cho việc trao đổi các dữ liệu này mà không tốn nhiều công sức mà thông thường phải bỏ ra để giữ được tính bí mật.

4.2. Mật mã có khoá công khai RSA

Là một trong những hệ mật mã có khoá công khai ra đời đầu tiên do các tác giả Rivest, Shamir và Adleman. Trong phương pháp này, việc mã hóa và giải mã dùng hàm luỹ thừa:

$$y = x^e \text{ Mod } m, \text{ và } \quad x = y^d \text{ Mod } m$$

Trong đó: x là đoạn tin, e là khoá công khai được sử dụng để mã hoá, y là đoạn tin đã được mã hoá, d là khoá bí mật dùng để giải mã

Thuật toán sử dụng trong RSA dựa trên nguyên lý: nếu có 2 số nguyên tố lớn p và q, ta có thể dễ dàng tính m = p. q, nhưng để làm ngược lại, khi biết m ta khó mà có thể giải ra hai số p và q.

Thực ra thì cũng không phải là một bài toán khó đối với kẻ xâm nhập khi mà p và q không phải là số nguyên tố lớn, vì thế thông thường người ta thường chọn hai số p và q lớn nếu có thể, miễn là có thể tính toán đủ nhanh.

Nếu chu kỳ là β, định lý Fermat thừa nhận rằng, với mọi x ta có:

$$x^{\beta+1} = x \text{ Mod } m$$

Nếu $e.d = 1 \text{ Mod } \beta$

Thì $x = y^d = (x^e)^d = x^{ed} \text{ Mod } m$

Chẳng hạn nếu chu kỳ lặp lại là β = 4, m= 15, e = 3 => d = 5, và hàm mã hoá sẽ là:

$y = x^3$, và $x = x^9$ vì ta sẽ có 9 = 1 Mod 4

Các bước thực hiện việc mật mã được tiến hành như sau:

a. Chọn hai số nguyên tố p, q lớn (tại USA hiện đang sử dụng $p, q > 10^{150}$)

   Tính m = p . q

   Tính β = BSCNN (p-1) (q-1)

b. Tìm số d thoả mãn điều kiện UCLN (d, β) = 1, thông thường chọn d thuộc đoạn [max (p, q) +1, m-1] vì nếu chọn d nhỏ quá thì càng ít giá trị của d để kẻ xâm nhập có thể thử.

c. tính e thoả mãn biểu thức ed%β = 1 (phép chia lấy dư)

d. Thực hiện mã hoá $y = x^e \text{ Mod } m$

Việc tính toán chọn lựa này được thực hiện ở bên thu (bên cần nhận bản tin), sau đó gửi e và m sang cho bên cần gửi bản tin

Ví dụ cụ thể: Để đơn giản ta lấy một ví dụ với số nhỏ

Bên sẽ nhận bản tin thực hiện:

1. Giả sử chọn hai số 5 và 11 là hai số nguyên tố

   p = 5, q = 11.

2. Tính m = p . q

   = 5 . 11 = 55

3. tính p-1, q - 1

   p - 1 = 5 - 1 = 4

   q - 1 = 11 - 1 = 10

4. Tính β = BSCNN (4 , 10) = 20

5. Lấy một số 81 = 1 Mod 20

6. Ta có thể chọn d = 9, e =9 => ed = 81;

7. Gửi e = 9, đồng thời với truyền m = 55 sang cho bên cần gửi bản tin.

Bên sẽ gửi bản tin thực hiện:

8. Mã hoá đoạn tin x cho bên nhận do tính lặp lại ta có

   $y = x^e \text{ Mod } 55$

   Giả thiết: x=2

   $y = 2^9 = 512 \% 55 = 17$

   (Giá trị y = 17 được gửi cho bên nhận)

9. Sau khi bên nhận đã nhận được y= 17 tiến hành giải mã.

   $x = y^d = 17^9 \text{ Mod } 55 = 118587876497\%55 = 2$

Kết quả nhận được đúng với đoạn tin đã gửi đi: x= 2.

Như ta thấy rằng chỉ cần bên nhận gửi một số e = 9, m= 55 thì nó sẽ nhận được y = 17 và giải ra thì nó là x= 2, trong khi đó kẻ phá hoại chỉ có trong tay khi thu được e = 9, m=55 và nhận được y = 17 trên đường truyền vật lý vì không biết p và q nên không thể biết được β và do vậy cũng chẳng thể suy ra được d, và thật khó có thể biết đó là 2 đã được mật mã hoá. Như vậy nếu p và q được giữ bí mật thì việc khai thác của kẻ xâm nhập trong trường hợp này là cực kỳ khó khăn vì không thể dò ra khoá giải mã.

❖ *Đánh giá độ bảo mật của phép mật mã RSA*

Theo đánh giá phép mật mã RSA có 5 ưu điểm sau của hệ mật mã hiện đại:

1. Độ bảo mật cao (nếu dùng phương pháp thám mã đòi hỏi thời gian rất lớn)
2. Thao tác nhanh (thao tác mã hoá và giải mã tốn ít thời gian)
3. Dùng chung được
4. Có thể ứng dụng rộng dãi
5. Có thể ứng dụng cho chữ ký điện tử

Phương pháp RSA đã có rất nhiều người tìm cách khai thác, tìm hiểu nhằm tìm ra kẽ hở để có thể khai thác. Một trong các phương pháp đó là dựa vào bản tin đã mã hoá và khóa công khai đã biết để suy luận bản tin rõ. Việc suy luận theo phương pháp thông thường được chứng minh cần ít nhất p hoặc q pha (hay lần thử), và điều quan trọng hơn là để thực hiện một một phép thử cần rất nhiều phép tính toán => cần rất nhiều thời gian

Có một phương pháp khác để phá, đó là phương pháp lặp là phương pháp cứ cho mũ e thật nhiều lần số y (dựa vào các số thu được) sau một số lần xuất hiện thì nó sẽ là giá trị x, cụ thể được ví dụ như sau:

Giả sử kẻ xâm nhập có thể thu được y = 3 và bắt được e = 9 là mã khoá công khai và tiến hành thử trên modulo 23. Phép mã hóa lặp lại nhiều lần sẽ được kết quả như sau:

$3^9 = 18 \text{ Mod } 23$

$18^9 = 12 \text{ Mod } 23$

$12^9 = 4 \text{ Mod } 23$

$4^9 = 13 \text{ Mod } 23$

$13^9 = 3 \text{ Mod } 23$

Đến đây việc giải mã đã có thể kết thúc! chỉ sau có 5 pha tính toán vì $13^9 = 3$ vì thế dữ liệu ban đầu là 13. Nếu như số chu trình chỉ có một số pha (vừa phải) thì kẻ xâm nhập hoàn toàn có thể giải thành công.

Nhưng Rivest đã phân tích độ dài chu trình cho phương pháp lặp đó và chỉ ra rằng, có những điều kiện đơn giản trên các số nguyên tố p và q trở thành phương pháp không thể thực hiện việc dò được. Tiêu chuẩn đó là: chọn kích thước m sao cho đảm bảo rằng: bằng thuật toán logarit không thể xâm nhập theo kiểu phép tính $d = \log_y x$ (tức là nếu thử bằng cách luỹ thừa liên tiếp như trên) và bằng phép phân tích thành thừa số cũng không thể xâm nhập, ngoại trừ phải thực hiện một phép toán khổng lồ (mà điều này là không thể vì nó đòi hỏi mất nhiều thời gian đối với kẻ xâm nhập)

Thuật toán RSA có ý nghĩa quan trọng trong ứng dụng thực tế vì độ phức tạp của phép phân tích thành thừa số, nó không thể xác định được bằng cách tìm thuật toán tốt nhất và bằng cách tính toán độ phức tạp của nó.

Thuật toán RSA đang chiếm vị trí quan trọng trong các dạng mật mã có khóa công khai và chữ ký số. Trong WCDMA, RSA được ứng dụng trong việc thực hiện bảo mật thông tin cần truyền, và trong ứng dụng vào các thuật toán nhận thực.

4.3. Các thuật toán Băm (Hàm Hash)

Vấn đề:

Như ta đã biết, trong truyền thông nhận biết được nơi gửi, nơi nhận thôi thì chưa đủ, kẻ xâm nhập có thể thu lại bản tin đó và thêm vào, bớt đi hoặc đơn giản là thay đổi vị trí các bit cho nhau, sau đó gửi tiếp nó trên đường truyền.

Ví dụ: Công ty A gửi một biên bản yêu cầu ngân hàng rút 1000 $ từ tài khoản của công ty cho B, nhưng trên đường truyền nó có thể bị chặn lại và sửa đổi nội dung từ 1000 $ thành 10.000 $, hoặc không phải cho B mà lại là cho C, bằng phương pháp thông thường chỉ có thể giải ra thì vẫn chưa đủ để xác nhận các con số, hoặc dữ liệu nhận được là chính xác, vì vậy cần có một phương pháp để biết chính xác bản tin nhận được đã bị sửa đổi hay chưa.

Các thuật toán thực hiện công việc này đều dựa trên cơ sở hàm một phía (hay hàm một chiều (one-way function).

Hàm một phía:

- Có thế tính theo chiều thuận $y = f(x)$ một cách dễ dàng.

- Tính theo chiều ngược lại $x = f^{-1}(y)$ thì lại rất khó khăn.

Ví dụ:

$y = f(x) = a^x \text{ Mod } n$ là hàm một phía

vì: Tính xuôi $y = f(x) = a^x \text{ Mod } n$ dễ

Tính ngược $x = \log_a y \text{ Mod } n$ khó

Khi a là phần tử được giữ bí mật, và N là số nguyên tố lớn.

Hàm một phía có cửa sập:

Hàm y = f(x) được định nghĩa là hàm một phía có cửa sập nếu tính xuôi thì dễ nhưng tính ngược thì khó, tuy nhiên bài toán đó trở nên dễ nếu như biết cửa sập.

Điển hình trong số các hàm cửa sập là hàm Hash. Một hàm Hash được biết như là một hàm băm, chính vì vậy thuật ngữ hàm băm hay hàm Hash có thể được thay thế cho nhau. Một hàm Hash nhận một bản tin M có chiều dài bất kỳ và chuyển nó thành một kết quả H(M) có chiều dài cố định tại đầu ra. Thông thường thì H(M) rất nhỏ so với M; ví dụ H(M) có thể chỉ 18, 64, hoặc 128 bit, trong khi M có thể có độ dài tới vài Mega byte hoặc hơn.

Có thể hiểu hàm băm là hàm một chiều. Ví dụ như hàm nhân hai số lớn thành một tích mà khi biết được tích của nó thì khó mà có thể suy ra hai số lớn ban đầu, hoặc biết một dãy các số, thường là dãy số siêu tăng (Super Increasing Sequence), có thể suy ra tổng S của nó dễ dàng, nhưng khi biết tổng S của nó thì khó mà biết được nó được cộng từ những số nào, nhất là đối với số lớn.

Trong nhận thực, hàm băm thường đóng một vai trò hết sức quan trọng, vì thế cho nên là rất hữu ích nếu chúng ta biết được các tính chất sau đây:

1. Một hàm Hash có thể thực hiện biến đổi với các khối dữ liệu M đầu vào có độ dài biến đổi
2. Một hàm Hash chỉ tạo ra một mã băm có độ dài cố định H(M)
3. H(M) phải được tính toán cho bất kỳ một bản tin M nào khi có yêu cầu nhận thực trên bản tin đó.
4. Không thể tính toán để tìm ra được bản tin M khi biết được H(M) hay nói cách khác nó không thể tính ngược bởi một kẻ xâm nhập.
5. Đối với bất kỳ bản tin M nào, một hàm Hash phải đảm bảo không thể tìm ra một bản tin M' mà bản tin đó có H(M') = H(M). Nói cách khác nó phải đảm bảo không thể tìm ra hai bản tin khác nhau M và M', $M \neq M'$, mà chúng ánh

xạ ra cùng một giá trị H(M) = H(M'). Một hàm thoả mãn điều kiện này gọi là hàm Hash chống xung đột.

Đúng theo nghĩa đen của nó, hàm Băm thực hiện "băm " dữ liệu ra, tất nhiên là theo một thuật toán cho trước và đã được tính toán và thêm vào đó chữ ký để có thể kiểm tra. Các thuật toán hàm băm thường gặp trong thực tế là thuật toán MD2 (Kaliski), thuật toán MD5 (Rivest), và thuật toán băm có bảo mật (NIST).

Trong phương pháp hàm băm, ở phía nhận cũng thực hiện phép toán tương tự như bên gửi. Ở trong phương pháp của chúng ta, bằng các phương pháp mật mã hoá đã nêu ở trên có thể đảm bảo được rằng, mặc dù dấu xác thực gửi kèm với bản tin nên vẫn có thể bị thu được trên đường truyền, nhưng vì bản thân tất cả các bit truyền đi đều không thể giải được bởi kẻ xâm nhập nên chúng chỉ có thể xen vào bản tin các bit hoặc xáo trộn các bit. Các kết quả tính toán sẽ được so sánh với dấu xác thực sau khi giải mã. Nếu so sánh phù hợp thì xem như dữ liệu trao đổi giữa hai bên trao đổi không thay đổi và khẳng định đó là bản tin đúng. Còn nếu kết quả không phù hợp thì có nghĩa là bản tin đã bị thay đổi.

Một hàm băm sẽ nhận một thông báo có độ dài và trật tự biết trước để cho ra ở đầu ra một dữ liệu có chiều dài cố định, khi có sự thêm hoặc bớt một bit hay một ký tự sẽ gây nên sự thay đổi ở đầu ra của hàm băm. Cũng như vậy sự tráo đổi lẫn nhau giữa các bit hoặc ký tự trong thông báo cũng gây ra sự thay đổi ở đầu ra.

Ví dụ: Phương pháp kiểm lỗi CRC là một ví dụ điển hình trong đó trường kiểm lỗi được truyền cùng với dữ liệu, và cả dữ liệu được chia cho hàm sinh để tìm ra các bit cho trường kiểm lỗi, ta thấy chỉ cần cho thêm một bit vào, bớt một bit đi hoặc đảo lộn vị trí giữa chúng lập tức chúng ta phát hiện ra là trường kiểm lỗi không còn phù hợp nếu nó vẫn giữ nguyên như cũ.

Một vấn đề được đặt ra là vì hàm băm ánh xạ thông báo có độ dài bất kỳ thành dấu xác thực có chiều dài cố định, như vậy có thể có câu hỏi đặt ra là liệu như thế khi có một thay đổi về số lượng bit hoặc xáo trộn các bit trong bản tin mà vẫn cho ra được một dấu xác thực giống nhau thì sao? Vấn đề này có phương án giải quyết như sau:

- Làm cho không gian dấu xác thực đủ lớn để cho các thông báo khác sẽ tương ứng với các dấu xác thực khác nhau, tuy nhiên vẫn phải có trường hợp hai thông báo khác nhau cho ra một dấu xác thực, do không gian dấu xác thực không thể lớn vô cùng được, trong khi các thông báo thì hầu như cái nào cũng khác nhau.

- Về phía thuật toán băm sẽ đảm bảo rằng các thông báo cho ra cùng tạo ra một dấu xác thực sẽ khác xa nhau sao cho từ một thông báo ta không thể sửa thành thông báo kia.

Trong lĩnh vực tài chính thì khối dấu xác thực dùng 32 bit (tức là $2^{32} = 42.10^8$ khả năng).

Bây giờ chúng ta xem xét một thuật toán băm điển hình:

4.3.1. Thuật toán băm MD5

Thuật toán MD5 là thuật toán được sử dụng tương đối phổ biến trong thực tế để kiểm tra tính toàn vẹn của các khối dữ liệu lớn. Thuật toán nhận đầu vào là một bản tin có chiều dài bất kỳ, xử lý nó thành các khối 512 bit và tạo ra đầu ra là một đoạn tin 128 bit. Quá trình thực hiện bao gồm các bước sau:

1. Đoạn tin ban đầu được nhồi thêm (cộng thêm) một số bit (bit bắt đầu là 1 còn các bit sau là 0, số bit được thêm vào có thể từ 1 đến 512 bit), sao cho tổng số bit của đoạn tin (sau khi cộng thêm các giá trị khởi đầu là 64 bit) sẽ là bội số của 512.
2. Khởi tạo bộ đệm MD. Đó là các bộ đệm 128 bit được sử dụng để chứa kết quả trung gian và cuối cùng của hàm băm. Có thể xem bộ đệm như bốn thanh ghi 32 bit. Các thanh ghi này được khởi tạo (ở hệ Hex) như sau:

   A = 0 1 2 3 4 5 6 7; B = 8 9 a b c d e f;

   C = f e d c b a 9 8; D = 7 6 5 4 3 2 1 0;
3. Xử lý các đoạn tin thành từng khối 512 bit (chia thành 16 từ, mỗi từ 32 bit). Quá trình tính toán được chia thành từng giai đoạn, số giai đoạn bằng chiều dài tính theo bit của đoạn tin sau khi đã được nhồi thêm chia cho 512. Mỗi giai đoạn thực hiện trong bốn vòng, các có cấu trúc giống nhau nhưng mỗi vòng sử dụng một hàm logic khác nhau, được đặc trưng bởi sự kết hợp các thông số đặc trưng và phối hợp sử dụng các hàm biến đổi.
4. Đoạn tin đầu ra có độ dài là 128 bit chính là dấu nhận thực đặc trưng cho đoạn tin.

   Có thể tóm tắt hoạt động của thuật toán MD5 như sau:

   $MD_o = IV$

   $MD_{q+1} = MD_q + f_I(Y_q, f_H(Y_q, f_G(Y_q, f_F(Y_q, MD_q))))$

$MD = MD_{L-1}$

Trong đó:

IV: chính là khối khởi đầu ABCD đã được xác định ở bước 2

Y_q là khối tin 512 bit thứ q

L là chiều dài của đoạn tin (đã được nhồi thêm)

MD là giá trị cuối cùng

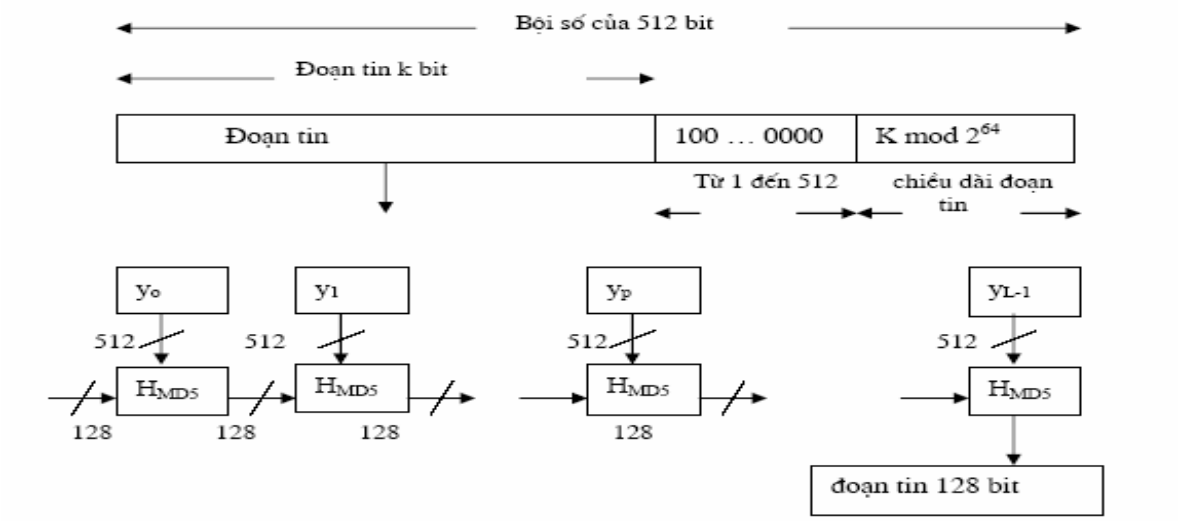
f_i là các hàm :

F (b, c, d) = (b*c) | (b*d)

G (b, c, d) = (b*d) | (c*d)

H (b, c, d) = b ⊕ c ⊕ d

I (b, c, d) = c ⊕ (b*d)



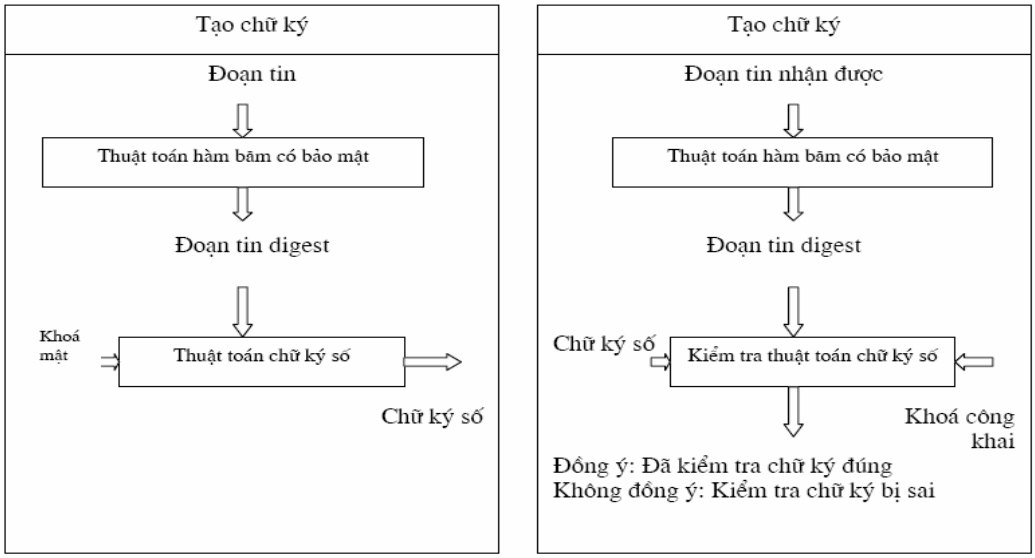
Hình 4.14. Tạo đoạn sử dụng thuật toán MD5

H_{MD5} là thuật toán sử dụng để băm 512 bit tạo ra 128 bit

Ta thấy rằng chỉ với 128 bit nhưng ta có thể nhận biết được các bản tin khác nhau sẽ tạo ra các dấu xác thực khác nhau bằng cách tổ hợp các bit này với nhau, theo lý thuyết có $2^{128} = 3.4\ 10^{38}$ các dấu xác thực khác nhau, tuy lớn nhưng nó cũng không phải là con số vô cùng, tuy nhiên sự kết hợp của thuật toán đảm bảo rằng các bản tin cho ra cùng một dấu xác thực là rất khác nhau.

4.3.2. Thuật toán băm có bảo mật SHA

Trong thuật toán này kết quả đầu ra là một dấu nhận thực 160 bit được gọi là *đoạn tin thu gọn*. Một khoá mật tăng cường được sử dụng như một chữ ký. Giữa thuật toán chữ ký số DSA (digital signature algorithm) và thuật toán băm có bảo mật SHA (Secure Hashing Algorithm) có một đoạn tin được xác thực của độ toàn vẹn đã được biết trước được tạo ra. Tại phía thu, thuật toán SHA được thực hiện trên đoạn tin và cũng tạo ra ở đầu ra đoạn tin digest. Nếu như kết quả băm đó là giống và chữ ký được kiểm tra (ở phía thu sử dụng một khoá công khai để kiểm tra), thì như vậy đoạn tin là được xác thực đúng người gửi và đã có bảo toàn dữ liệu



Hình 4.15. Thuật toán băm và chữ ký số

Ở đây đã có sự kết hợp giữa hàm băm và chữ ký số, khi mà hàm băm được thực hiện trên dữ liệu đã bị thay đổi sẽ dẫn đến sai cả *đoạn tin thu gọn* lẫn chữ ký số và việc kiểm tra chữ ký số được thực hiện bằng một mã khoá công khai.

Ta thấy rằng với hàm Hash và các thuật toán dựa trên cơ sở các dạng khác nhau của hàm một phía là cơ sở toán học cho chúng ta tiến hành kiểm tra tính toàn vẹn của một bản tin cần xác thực. Với tính chất một bản tin thì thu được một mã băm duy nhất, đây chính là điều chúng ta cần có để rút ra kết luận về tính chất của nơi tạo ra các bản tin này thông qua các thông số mật. Trong hệ thống WCDMA thuật toán nhận thực cũng sẽ dựa vào các hàm một chiều như thế này để thực hiện việc xác nhận.

Đây là các thuật toán quan trọng làm cơ sở để thực hiện việc nhận thực và bảo mật thông tin trong hệ thống thông tin di động WCDMA

Chương 5: Nhận thực và bảo mật trong hệ thống WCDMA

Với tất cả các lý do nêu trên, các đòi hỏi phải bảo mật và đảm bảo tuyệt đối an toàn đối với dữ liệu, đồng thời với các cơ sở thuật toán, các cấu trúc hệ thống đã xét chúng ta có thể xem xét kỹ thuật nhận thực và bảo mật trong hệ thống WCDMA.

Rõ ràng để có thể đảm bảo rằng người truy cập có thiết bị được coi là hợp lệ khi và chỉ khi thiết bị đó đã được mạng biết trước. Bằng cách mạng lưu các cơ sở dữ liệu liên quan đến thiết bị thuê bao đó, và chính bản thuê bao MS cũng phải có đủ cơ sở dữ liệu của riêng mình để chứng tỏ với mạng rằng: ‘ tôi ‘ cũng có những kết quả khớp hoàn toàn với kết quả mà ‘ngài ‘ có. Các số liệu này tất nhiên phải có một kỹ thuật lưu trữ đặc biệt, chúng chỉ có thể được giải mã bởi kỹ thuật cao mà người bình thường không dễ có được, đồng thời phải có những thuật toán đặc biệt để nhận dạng các số liệu này là duy nhất trên một thuê bao.

Thêm vào đó, bên cạnh các số liệu cố định không đổi, còn có các cơ sở dữ liệu (CSDL) cập nhật (hay còn gọi là các số bán cố định), và mang tính ngẫu nhiên đủ lớn, để các CSDL lưu trữ luôn đổi mới. Đặc điểm này cho phép cho dù có kỹ thuật tinh vi có thể đọc được các CSDL cố định, song cũng cần phải biết được chính xác bộ số bán cố định thì mới có thể liên kết với BS. Hiển nhiên là các thông số này cũng sẽ được bảo mật hoàn toàn khi chúng được truyền trên kênh truyền bằng cách sử dụng các kỹ thuật mã khối, mã dòng … hoặc không truyền chúng mà chỉ dùng chúng như là số liệu đầu vào để thực hiện tính toán và sau đó truyền các kết quả đã mã hoá trên kênh truyền. Như vậy phần nào đó chúng ta đã vẽ ra một bức tranh tương đối sáng sủa về sự nhận thực và sự bảo đảm an toàn trong hệ thống WCDMA. Trước hết ta xem xét xem những thông tin lưu trữ và đó cũng chính là cơ sở dữ liệu để thực hiện nhận thực và bảo mật.

5.1. Các cơ sở dữ liệu sử dụng cho quá trình nhận thực

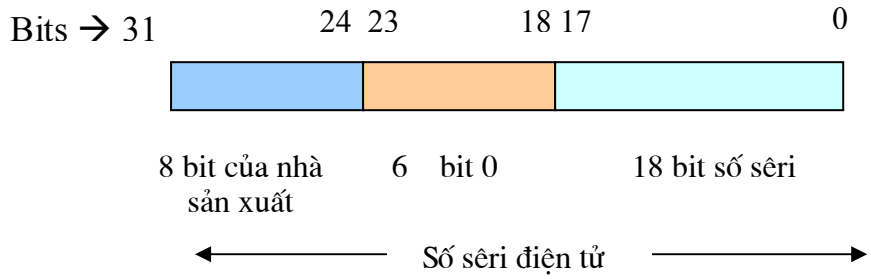
a. Khoá A (Authetication key)

Để nhận thực một MS, cần sử dụng khoá A (A- key), khoá A là một mẫu bí mật 64 bit được ấn định và lưu trữ trong bộ nhớ nhận dạng và an toàn vĩnh cửu của MS, và tại trung tâm nhận thực AUC của MSC chủ (MSC tại nơi MS đăng ký). Chỉ có AUC của hệ thống MSC chủ và MS là biết được khoá này, đây là phần bí mật nhất của số liệu bí mật. Khoá A và một số ngẫu nhiên đặc biệt (RANDSSD) có thể được AUC và MS sử dụng để tạo ra số liệu bí mật chung SSD (Shared Secret Data). AUC có thể phát SSD và các CSDL bí mật khác đến hệ thống đang phục vụ là MSC mới - hệ thống có AUC đòi hỏi phải các CSDL bí mật cho quá trình nhận thực - bảo mật, nhưng không

bao giờ phát các CSDL này vào không gian (điều này được thực hiện qua mạng liên kết các tổng đài). Không thực hiện trao đổi khoá A với MSC khác.

b. Số sêri điện tử : ESN

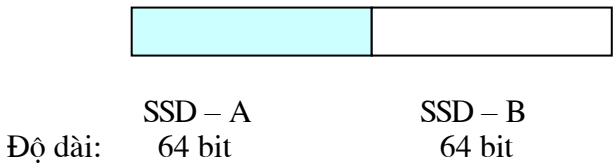
Mọi MS đều được ấn định trước một ESN khi chúng được sản xuất. ESN là một trường 32 bit xác định duy nhất MS trong hệ thống. Nó được đặt tại nhà máy sản xuất và rất khó có thể thay đổi được, nếu muốn thay đổi cần các kỹ thuật đặc biệt và bình thường thuê bao không thể có, các mạch chế tạo ESN phải được giữ bí mật với các kẻ phá hoại và ăn cắp, kể cả thiết bị gắn trên bo mạch hay cáp nối trên MS có liên quan cũng phải đảm bảo được điều này, nếu có bất kỳ một sự cố ý thay đổi nào thì điều đó sẽ làm cho MS đó lập tức ngừng hoạt động. Cấu trúc của ESN được mô tả trên hình dưới đây, trong đó 8 bit có trọng số lớn nhất 31 -> 24 của 32 bit là mã nhà sản xuất, từ bit 23 -> 18 là các bit dự phòng được đặt là 0, và các bit cuối cùng 17 -> 0 được dàng riêng cho mỗi nhà sản xuất để các nhà sản xuất lấy các tổ hợp các bit này để gán cho một MS hay một trạm di động duy nhất, khi các tổ hợp còn thiếu các nhà sản xuất sẽ được xem xét sử dụng trường dự trữ.



Hình 5.1. Cấu trúc của ESN

c. SSD : (Shared Secret Data)

SSD là một mẫu 128 bit được lưu trữ trong bộ nhớ bán cố định của MS và được AUC của MSC chủ biết. Như biểu diễn trên hình dưới đây, SSD được chia thành hai bộ số con tách biệt nhau, mỗi bộ số con cung cấp cho một thủ tục khác nhau. 64 bit SSD–A được dùng để thực hiện thủ tục nhận thực còn 64 bit SSD-B được sử dụng để thực hiện mật thoại và bảo mật bản tin của WCDMA.



Hình 5.2. Sự phân chia vùng SSD

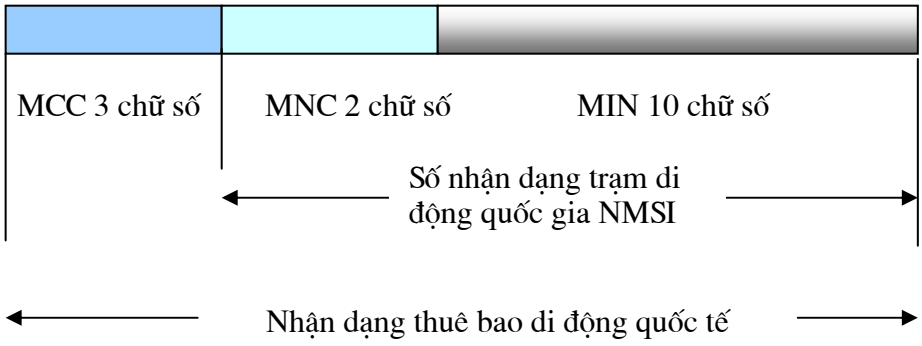
SSD được duy trì trong thời gian tắt nguồn. Nó được tạo ra bằng cách sử dụng số ngẫu nhiên 56 bit (RANDSSD do AUC của nơi đăng ký tạo ra), khoá A của MS, và ESN. Khi MS chuyển mạng không cần chuyển khoá A từ hệ thống này đến hệ thống khác. Các cập nhật SSD chỉ được thực hiện ở MS và HLR/AUC chủ nhà của nó chứ không thực hiện ở hệ thống đang phục vụ (MSC chủ nhà sẽ gửi số này qua mạng thông báo cho hệ thống khách). AUC quản lý các khoá mật mã liên quan đến từng thuê bao khi các chức năng này được cung cấp trong hệ thống.

d. *Bộ nhớ ngẫu nhiên RAND*

RAND là một số ngẫu nhiên 32 bit lưu trữ tại MS. RAND được BS phát đi định kỳ ở số liệu cập nhật hệ thống theo hai đoạn 16 bit: RAND–A và RAND–B trên kênh tìm gọi để cho MS cập nhật. MS sẽ lưu giữ và sử dụng phiên bản mới nhất của RAND trong quá trình để truyền tới BS trên kênh truy nhập. RAND của hệ thống hiện thời có thể khác với RAND mà MS sử dụng khi BS nhận được khi MS truy nhập mạng. Như vậy giá trị của RAND bằng giá trị thu được từ bản tin các thông số cuối cùng của kênh nhắn tìm. Các giá trị RAND đều được mật mã hoá trước khi truyền đi. Đây là một trong số CSDL bán cố định của hệ thống.

e. *IMSI: nhận dạng thuê bao quốc tế*

Số nhận dạng trạm di động (MSIN hoặc MIN) được định nghĩa theo số nhận dạng trạm thuê bao quốc tế (IMSI) trong khuyến nghị E.212 của ITU_T. IMSI là một trường 15 số. IMSI được chia làm hai phần, phần thứ nhất là mã nước di động MCC, phần thứ hai là số nhận dạng trạm di động quốc gia NMSI.



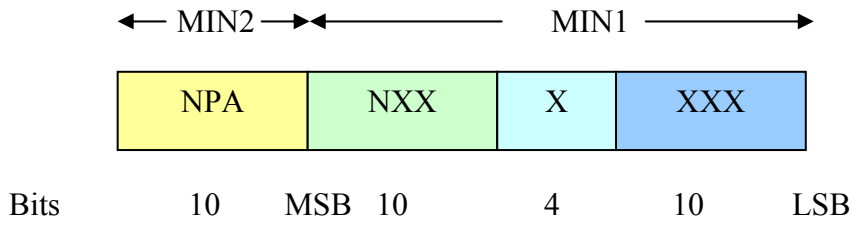
Hình 5.3 : Số nhận dạng trạm di động quốc tế (IMSI).

Theo chuẩn IMSI bao gồm một mã nhận dạng MCC 3 chữ số, một MNC (mã mạng di động) 2 chữ số và một MSIN (chỉ số nhận dạng trạm di động) 10 chữ số, các chữ số ở đây đều là cơ số 10.

Số nhận dạng trạm di động (MSIN hoặc MIN), được biểu diễn ở hình dưới đây, là một số 34 bit để hình thành 10 chữ số điện thoại.

10 chữ số điện thoại là: $D_1\ D_2\ D_3$ - $D_4\ D_5\ D_6$ - $D_7\ D_8\ D_9\ D_{10}$, trong đó $D_1\ D_2\ D_3$ là mã vùng, $D_4\ D_5\ D_6$ để chỉ trạm chuyển mạch, $D_7\ D_8\ D_9\ D_{10}$ để chỉ các số riêng cho từng MS

Trong đó các bộ số 10 số nhị phân đều được ánh xạ từ các bộ 3 số $D_1\ D_2\ D_3$, $D_4\ D_5\ D_6$, và $D_8\ D_9\ D_{10}$, theo bảng chuyển đổi thập phân thành nhị phân, 4 bit nhị phân được ánh xạ từ số D7 từ bảng chuyển đổi BCD.



Hình 5.4 : Số nhận dạng trạm di động (MIN hay MSIN)

Giả sử có một số điện thoại 10 chữ số là $D_1D_2D_3$-$D_4D_5D_6$-$D_7D_8D_9D_{10}$, trong đó $D_1D_2D_3$ biểu diễn mã vùng, $D_4D_5D_6$ biểu diễn trạm chuyển mạch, và $D_7D_8D_9D_{10}$ để chỉ một số thuê bao riêng biệt.

1. Ba chữ số đầu tiên được ánh xạ thành 10 bit (tương ứng với MSIN2) theo thuật toán mã như sau:
   - Biểu diễn 3 số $D_1\ D_2\ D_3$ như là các số độc lập
   - Tính toán $100\ D_1 + 10\ D_2 + D_3$ -111
   - Chuyển đổi kết quả tính toán được ở trên thành số nhị phân bằng cách sử dụng bảng chuyển đổi như ở hình dưới đây
2. Ba chữ số tiếp theo dược ánh xạ thành 10 bit của trường MSIN1 theo thuật toán tương tự ở trên
3. Bốn chữ số cuối cùng được ánh xạ thành 14 bit cuối của MSIN1(hay MIN1) theo cách như sau:

- Chữ số hàng nghìn được ánh xạ theo bảng chuyển đổi BCD, giống như bảng dưới đây.
- Ba chữ số cuối cùng được chuyển đổi thành 10 bit theo thuật toán tương tự như 1.

Chuyển ba số thập phân -> 10 bit		Chuyển đổi BCD	
Số thập phân	Số nhị phân	Số thập phân	Số nhị phân
1	0000 0000 01	1	0001
2	0000 0000 10	2	0010
3	0000 0000 11	3	0011
4	0000 0001 00	4	0100
5	0000 0001 01	5	0101
.	.	6	0110
.	.	7	0111
.	.	8	1000
998	1111 1001 10	9	1001
999	1111 1001 11	0	1010

Hình 5.5 Bảng biểu diễn chuyển đổi thập phân – nhị phân và chuyển đổi BCD

Ví dụ: chuyển đổi 10 chữ số điện thoại 290-453-7186 thành mã nhị phân MSIN2 (hay MIN2) và MSIN1 sử dụng các bước vừa nêu trên:

1. *Tính toán MSIN2*:

   10 bit của MSIN2 nhận được từ ba số đầu (hay là 290) của số điện thoại.

   - $D_1 = 2$, $D_2 = 9$ và $D_3 = 0$.
   - $100\ D_1 + 10\ D_2 + D_3 - 111 = 100\ (2) + 10\ (9) + 0 - 111 = 179$
   - 179 có mã nhị phân là ‘0010 1100 11’

2. *Tính toán MSIN1*:

   ❖ 10 bit có trọng số cao nhất của MSIN1 nhận được từ bộ ba số thứ hai của số điện thoại

   - $D_1 = 4$, $D_2 = 5$, và $D_3 = 3$.

- $100\ D_1 + 10\ D_2 + D_3 - 111 = 100\ (4) + 10\ (5) + 3 - 111 = 342$
- 342 trong mã nhị phân là : ‘ 0101 0101 10’

❖ Chuyển đổi BCD chữ số D_7: bốn bit nhị phân tiếp theo của MSIN1 nhận được từ việc chuyển đổi BCD chữ số hàng nghìn (hay 7) của số điện thoại.

- $D_7 = 7$ trong mã nhị phân là ‘0111’

❖ Tính toán ba chữ số cuối cùng (hay là $D_8D_9D_{10}$) của MSIN1: 10 bit có trọng số nhỏ nhất của nhận được từ 3 chữ số cuối cùng của số điện thoại

- $D_1 = 1$, $D_2 = 8$, và $D_3 = 6$
- $100\ D_1 + 10\ D_2 + D_3 - 111 = 100\ (1) + 10\ (8) + 6 - 111 = 75$
- 75 trong mã nhị phân là ‘ 0001 0010 11’

Như vậy MSIN1 sẽ là ‘0101 0101 1001 1100 0100 1011’

MNC được tính như sau:

1. Biểu diễn như các số riêng biệt 2 chữ số mã mạng di động D_1D_2, với chữ số 0 sẽ nhận giá trị 10
2. Tính toán: $10\ D_1 + D_2 - 11$.
3. Chuyển đổi thành nhị phân kết quả thu được từ bước theo bảng chuyển đổi trên.

Tính MCC:

1. Biểu diễn như các số riêng biệt các chữ số mã quốc gia $D_1\ D_2\ D_3$, với chữ số 0 sẽ nhận giá trị 10
2. Tính toán $100\ D_1 + 10\ D_2 + D_3 - 111$
3. Chuyển đổi nhị phân kết quả thu được từ bước 2 theo bảng chuyển đổi ở trên.

f. COUNT : Thông số lịch sử cuộc gọi

Thông số lịch sử gọi là một modul 64 bit được lưu trữ trong trạm di động MS. COUNT được trạm di động cập nhật khi MS nhận được bản tin cập nhật thông số trên kênh lưu lượng đường xuống WCDMA. Mỗi lần MS khởi xướng hay kết cuối cuộc gọi, đếm lịch sử lại tăng nên cả ở MS lẫn ở HLR của AUC hệ thống chủ. Bộ đếm này dùng để phát hiện sự nhân bản vì các nhân bản không có lịch sử gọi giống như MS hợp lệ.

g. TMSI: Nhận dạng di động tạm thời

TMSI là một số được ấn định tạm thời tại chỗ để đánh địa chỉ cho MS. MS nhận được TMSI khi nó được ấn định bởi BS (hay nút B). TMSI là chỉ số tạm thời để BS biết là MS đang có mặt trong sự quản lý của nó. Khi MS bật nguồn nó phải đăng ký với hệ thống. Khi đăng ký, nó phát IMSI của mình và số liệu khác tới mạng. Khi này EIR ở hệ thống khách hỏi HLR của hệ thống chủ thông tin tóm tắt về dịch vụ và các số liệu bảo mật. Sau đó EIR ấn định nhận dạng thuê bao di động tạm thời TMSI cho MS. MS sử dụng TMSI để truy nhập đến hệ thống.TMSI đảm bảo tính bảo mật thông tin vì chỉ MS và mạng biết nhận dạng MS thông qua TMSI. Khi MS chuyển mạng mới, một số giao diện không gian khác sử dụng TMSI để hỏi EIR cũ và sau đó ấn định TMSI mới cho MS.

5.2. Thủ tục nhận thực

Nhận thực trong WCDMA là thủ tục mà qua đó thông tin được trao đổi giữa MS và BS để nhằm mục đích khẳng định sự hợp lệ số nhận dạng của MS. MS phải cùng làm việc với hệ thống để thực hiện việc nhận thực. Quá trình nhận thực được thực hiện trên cơ sở dữ liệu lưu trên mạng và trên MS, bằng các thuật toán có đầu vào là các cơ sở dữ liệu này, nếu các kết quả tính toán hoàn toàn trùng nhau thì nhận thực thành công.

Tồn tại hai quá trình nhận thực chính: hiệu lệnh chung và hiệu lệnh riêng.

- *Hiệu lệnh chung*: Được khởi đầu ở kênh tìm gọi và truy nhập. Dùng hiệu lệnh chung MS có thể thực hiện các chức năng sau đây ở kênh truy nhập:
  - Nhận thực khi đăng ký.
  - Nhận thực khi khởi xướng cuộc gọi.
  - Nhận thực khi trả lời tìm gọi.
- *Hiệu lệnh riêng*: Được khởi đầu ở kênh lưu lượng đường xuống và kênh lưu lượng đường lên hoặc ở kênh tìm gọi và kênh truy nhập. BS khởi đầu nhận thực này khi nhận thực chung (gồm ba loại nhận thực trên) bị thất bại, hoặc một thời điểm bất kỳ sau khi nó đã ấn định kênh cho MS.

Các thông số đầu vào cho các thủ tục này được cho như trong bảng dưới đây:

Thủ tục nhận thực	Rand-Challenge	ESN	Số liệu nhận thực	SSD-AUTH	Các thanh ghi SAVE
Đăng ký	RAND	ESN	MSIN1	SSD-A	FALSE
Hiệu lệnh riêng	256 x RANDU + LSB của MSIN2	ESN	MSIN1	SSD-A	FALSE
Khởi xướng	RAND	ESN	MSIN1	SSD-A	TRUE
Kết cuối	RAND	ESN	MSIN1	SSD-A	TRUE
Hiệu lệnh trạm gốc	RANDBS	ESN	MSIN1	SSD-A-NEW	FALSE
Ấn định TMSI	RAND	ESN	MSIN1	SSD-A	FALSE

Hình 5.6 Bảng các thông số đầu vào cho các thủ tục nhận thực

Trong đó:

- RANDU: Biến ngẫu nhiên 24 bit
- RANDBS: Số liệu hiệu lệnh ngẫu nhiên 32 bit
- RAND: Giá trị hiệu lệnh nhận thực ngẫu nhiên (0 hoặc 32 bit)

a. Hiệu lệnh chung

Hiệu lệnh chung được thực hiện khi MS đăng ký, khởi xướng, và kết cuối cuộc gọi. Các thủ tục thực hiện nhận thực này như sau:

✓ MS thực hiện:

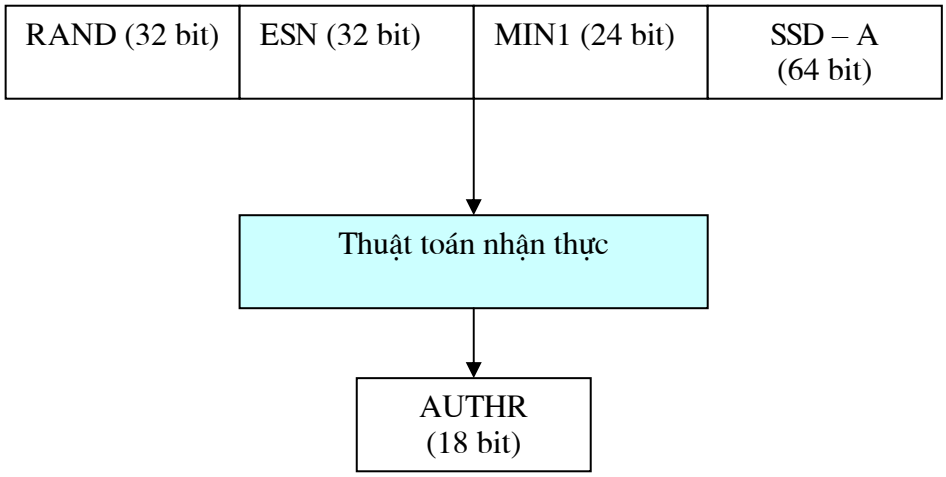
- Đặt các thông số đầu vào thủ tục nhận thực theo sơ đồ hình 5.7
- Đặt thông số đầu vào thanh ghi Save là FALSE
- Thực hiện các thủ tục nhận thực
- Đặt trường AUTHR (trường nhận thực) bằng 18 bit ra của thủ tục nhận thực
- Phát số liệu nhận thực (AUTHR) cùng với giá trị hiệu lệnh ngẫu nhiên RANDC (8 bit trọng số cao của RAND) và thông số lịch sử cuộc gọi (COUNT) đến BS thông qua bản tin trả lời nhận thực.

✓ BS thực hiện:

- So sánh giá trị RANDC thu được với 8 bit có trọng số cao nhất của RAND được lưu bởi hệ thống.

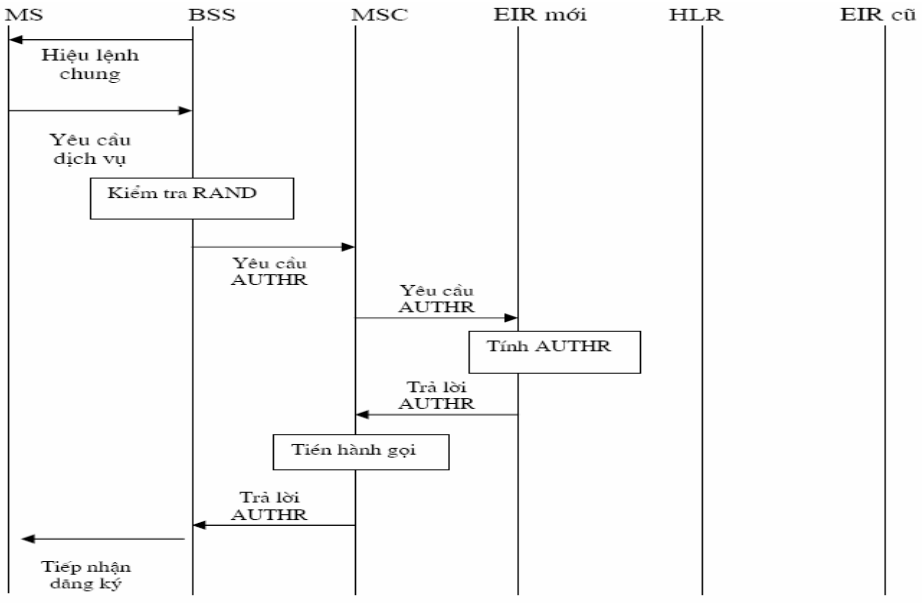
- So sánh giá trị COUNT thu được với giá trị COUNT được lưu trữ tương ứng với MSIN/ESN thu (nhằm xác định đúng số thuê bao và phù hợp hai chỉ số này).
- Tính toán AUTHR giống như MS nhưng sử dụng SSD-A được lưu của bản thân BS
- So sánh giá trị AUTHR tính được với AUTHR thu được

Nếu một trong số các so sánh ở BS thất bại, BS có thể cho rằng nhận thực thất bại và khởi đầu thủ tục trả lời hiệu lệnh riêng hay bắt đầu quá trình cập nhật SSD.



Hình 5.7 Tính toán AUTHR trong hiệu lệnh chung

Lưu đồ cho hiệu lệnh chung được mô tả ở hình sau:



Hình 5.8: Lưu đồ gọi cho hiệu lệnh chung.

Lưu ý:

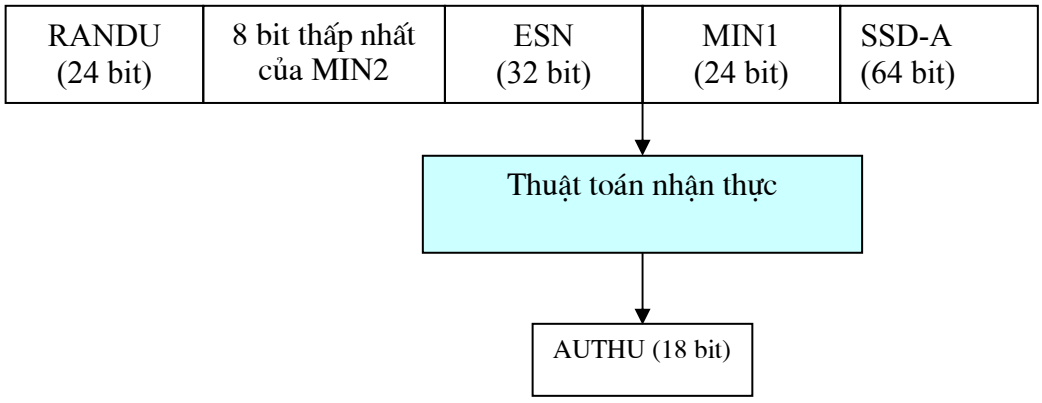
Đối với nhận thực khởi xướng thông số đầu vào MIN1 được thay thế bởi 24 bit tạo ra từ 6 chữ số được quay cuối cùng, nếu có ít hơn 6 chữ số trong bản tin khởi xướng, các bit có trọng số cao nhất của IMSI được sử dụng để thay thế các bit thiếu. Đối với nhận thực khởi xướng và nhận thực kết cuối MS đặt thông số đầu vào thanh ghi Save là TRUE thay vì FALSE như trong nhận thực đăng ký.

b. Hiệu lệnh riêng

BS thực hiện khởi đầu thủ tục trả lời hiệu lệnh riêng ở các kênh tìm gọi và truy nhập hoặc ở các kênh lưu lượng đường xuống và đường lên.

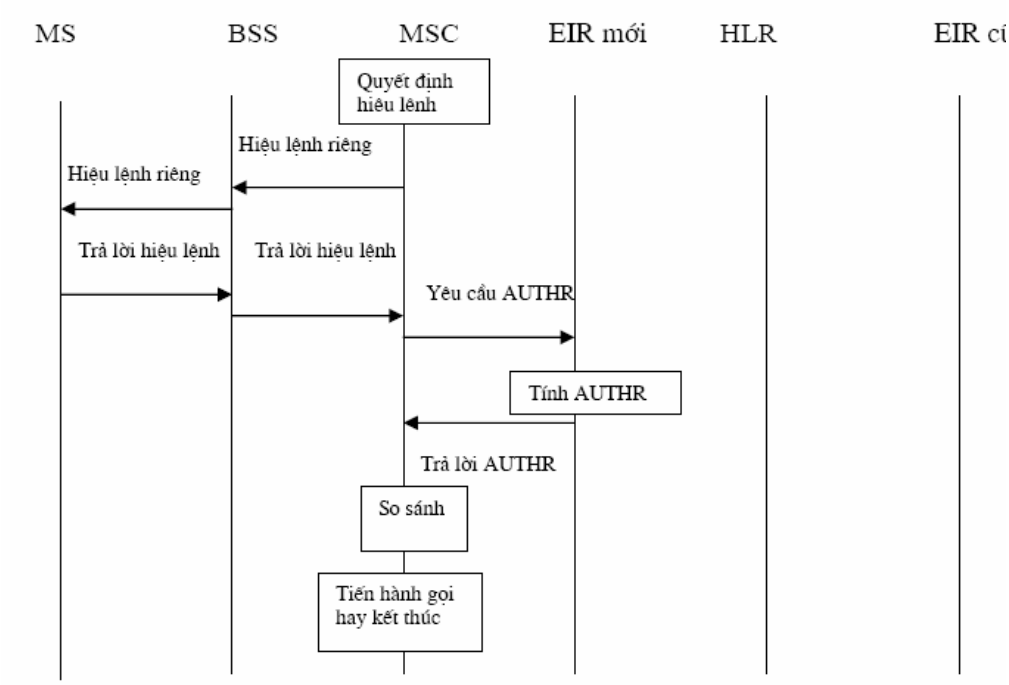
✓ BS thực hiện:

- Tạo ra số liệu ngẫu nhiên 24 bit (RANDU) và gửi nó đến MS thông qua bản tin hiệu lệnh riêng (hay bản tin nhận thực) ở kênh tìm gọi.
- Khởi đầu thuật toán nhận thực như hình 5.9
- Đặt AUTHU bằng 18 bit đầu ra của thuật toán nhận thực.



Hình 5.9. Tính toán AUTHU cho thủ tục trả lời hiệu lệnh riêng.

Lưu đồ cho hiệu lệnh riêng được mô tả như sau:



Hình 5.10 : Lưu đồ gọi cho hiệu lệnh riêng.

Khi MS nhận được bản tin yêu cầu hiệu lệnh riêng, MS thực hiện:

✓ MS thực hiện:

- Đặt các thông số đầu vào như hình 5.9
- Đặt thông số đầu vào thanh ghi Save là FALSE
- Tính toán AUTHU như trên nhưng sử dụng RANDU thu được và các thông số khác lưu trữ ở MS
- Gửi AUTHU đến trạm BS bằng bản tin trả lời hiệu lệnh riêng (trên một trong hai kênh nêu ở trên)

Dựa vào giá trị AUTHU nhận được từ MS, BS so sánh giá trị AUTHU của nó tính toán với giá trị nhận được từ MS. Nếu so sánh thất bại, BS có thể từ chối ý định truy nhập tiếp theo của MS, huỷ bỏ cuộc gọi đang tiến hành và khởi đầu quá trình cập nhật SSD.

c. Cập nhật SSD

Để có SSD mới, HLR/AUC sẽ khởi đầu thủ tục cập nhật cập nhật SSD. Quá trình thực hiện diễn ra như hình 5.11.

✓ BS thực hiện:

- Phát lệnh cập nhật trên kênh tìm gọi hoặc kênh lưu lượng đường xuống cùng với 56 bit của RANDSSD do HLR/AUC tạo ra đến MS thông qua bản tin cập nhật SSD.

Khi nhận được bản tin cập nhật SSD, MS sẽ:

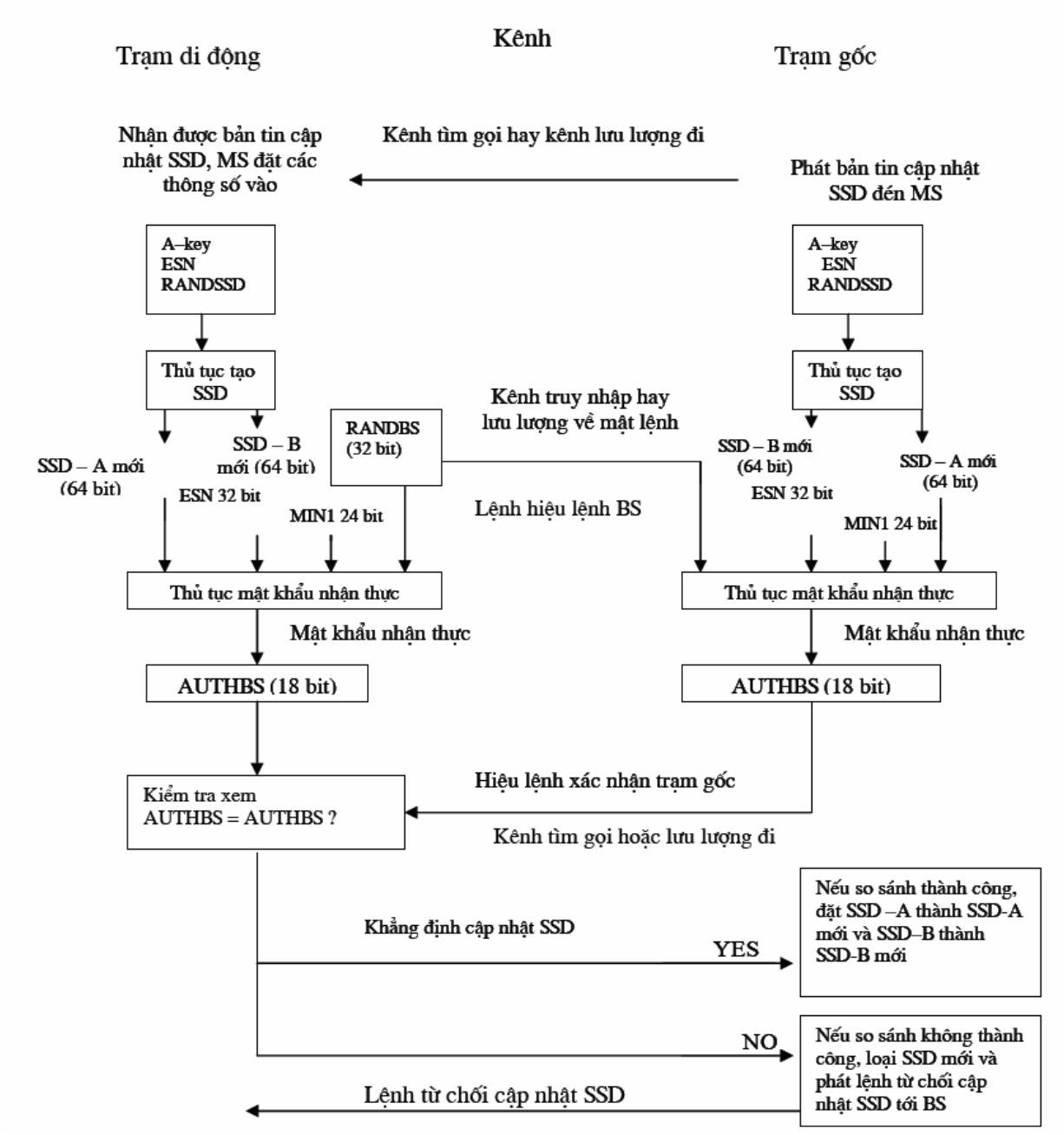
✓ MS thực hiện:

- Đặt các thông số đầu vào thủ tục tạo SSD (như hình 5.11).
- Thực hiện thủ tục tạo SSD.
- Tính toán 128 bit SSD-mới với 64 bit trọng số lớn là SSD-A mới và 64 bit trọng số nhỏ là SSD-B mới.
- Đặt các thông số đầu vào thuật toán nhận thực như hình 5.11
- Thực hiện thuật toán nhận thực.
- Chọn 32 bit ngẫu nhiên (RANDBS) và gửi nó đến BS ở lệnh hiệu lệnh BS trên kênh truy nhập hoặc kênh lưu lượng hướng lên
- Đặt AUTHBS bằng 18 bit nhận được từ thuật toán nhận thực.
- Đặt thông số đầu vào thanh ghi Save là FALSE.

Khi nhận được bản tin lệnh hiệu lệnh BS, BS sẽ:

✓ BS thực hiện:

- Đặt các thông số đầu vào thuật toán nhận thực với RANDBS thu được từ bản tin hiệu lệnh BS (như hình 5.11).
- Thực hiện thuật toán nhận thực.
- Đặt AUTHBS bằng 18 bit nhận được từ thuật toán nhận thực.
- Công nhận thu được bản tin hiệu lệnh BS bằng cách phát đi khẳng định hiệu lệnh BS chứa AUTHBS trên kênh tìm gọi hoặc kênh lưu lượng hướng thuận.



Hình 5.11. Thủ tục cập nhật SSD

Khi nhận được khẳng định hiệu lệnh BS, MS sẽ:

✓ MS thực hiện:

- So sánh AUTHBS thu được với AUTHBS do nó tính.
- Công nhận thu khẳng định hiệu lệnh BS theo cách sau:

  Nếu so sánh thành công:

+ Thực hiện cập nhật SSD-mới.

+ Phát khẳng định cập nhật SSD đến BS để chỉ thị rằng thực hiện thành công việc cập nhật SSD.

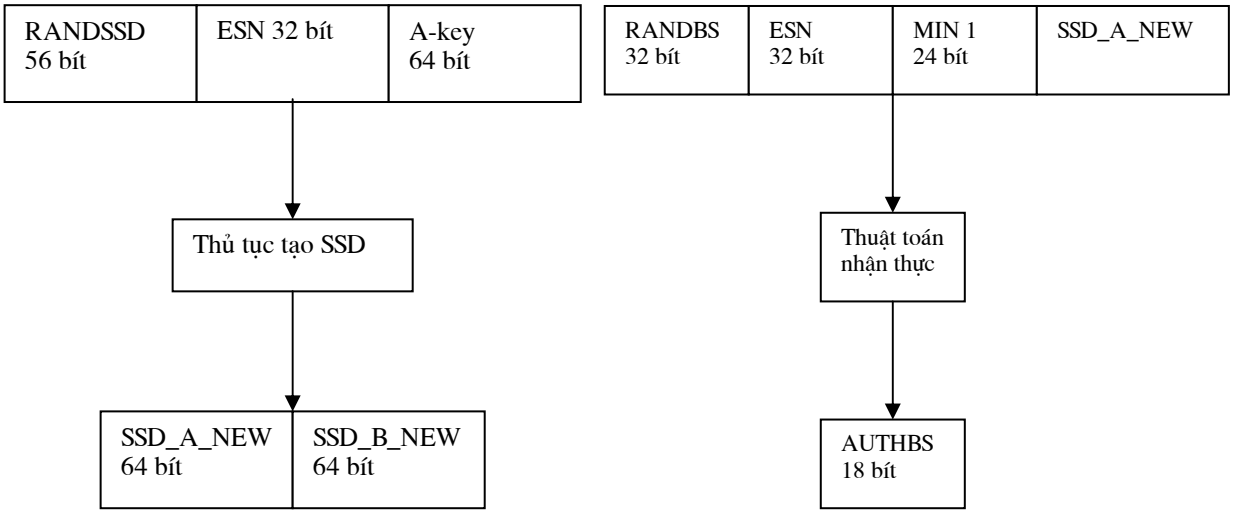
Nếu so sánh thất bại:

+ Huỷ SSD-mới.

+ Phát bản tin từ chối cập nhật SSD đến BS biểu thị rằng thực hiện cập nhật SSD không thành công.

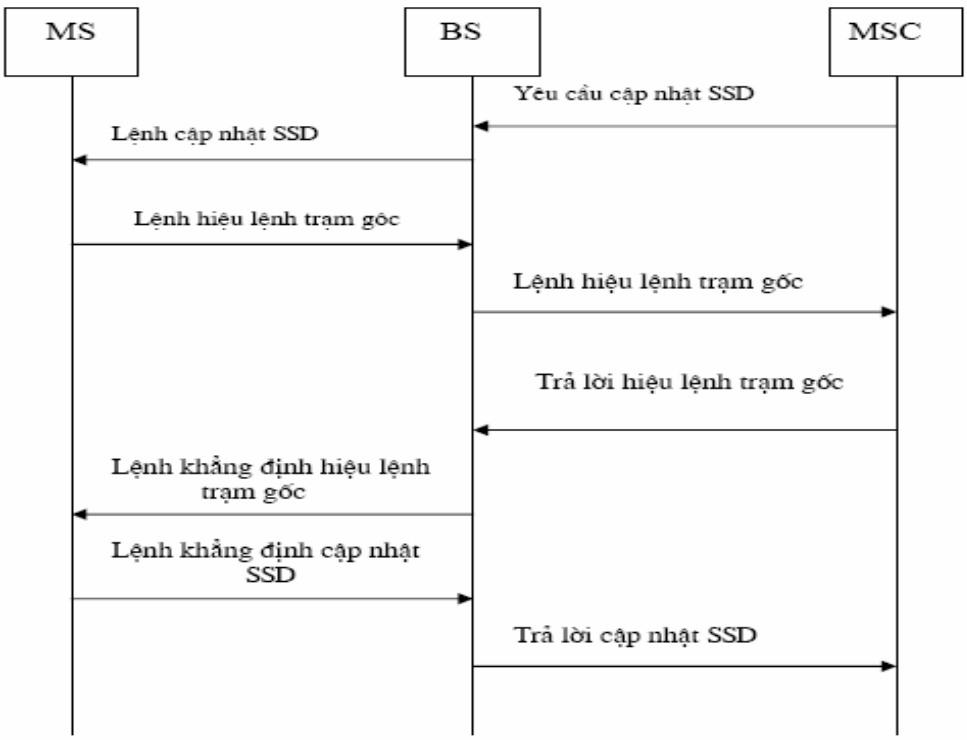
✓ Khi BS nhận được các bản tin từ MS, nếu bản tin nhận được từ MS chỉ ra rằng thực hiện thành công việc cập nhật tại MS thì HLR/AUC sẽ thực hiện cập nhật SSD, đặt SSD-A thành SSD-A-mới, và SSD-B thành SSD-B-mới. Trong trường hợp ngược lại tức là nhận được bản tin từ chối cập nhật của MS, hoặc sau một thời nhất định BS không nhận được tín hiệu trả lời của MS, HLR/AUC sẽ loại bỏ giá trị SSD-mới.

Trong sơ đồ trên các thuật toán tạo SSD và tính toán giá trị AUTHBS có các thông số đầu vào như sau:



Hình 5.12. Sơ đồ thực hiện tạo SSD và tính toán AUTHBS trong sơ đồ cập nhật

Lưu đồ thực hiện việc cập nhật SSD diễn ra như sau:



Hình 5.13 Lưu đồ cập nhật SSD

Với 3 thủ tục nói trên ta có thể thực hiện nhận thực với các quá trình đăng ký, khởi xướng cuộc gọi, cũng như kết cuối cuộc gọi một cách an toàn

Thông thường các thuật toán tính toán và so sánh ở phía BS được thực hiện ở AUC.

Nhận xét và giải pháp:

Như vậy tất cả các quá trình đăng ký, khởi xướng một cuộc gọi, hay khi trả lời tìm gọi (trả lời khi có người khác gọi đến MS) đều thông qua các hiệu lệnh trên. Một cuộc gọi sẽ được kiểm soát theo các bước như sau:

- Nếu hiệu lệnh chung bị thất bại thì có thể khởi động quá trình cập nhật SSD, hoặc khởi động hiệu lệnh riêng
- Nếu nhận thực riêng thất bại ta có thể huỷ bỏ ngay liên lạc của MS, hoặc khởi động quá trình cập nhật SSD
- Nếu cập nhật SSD bị sai ta có thể thử lại quá trình cập nhật này một số lần hữu hạn nhất định nếu tiếp tục sai thì ta buộc phải huỷ cuộc gọi.

Trong quá trình nhận thực thì cả MS và hệ thống mà cụ thể là MSC/VLR đều thực hiện tính toán từ CSDL cố định và bán cố định.

Đồng thời cũng có thấy rằng hiệu lệnh riêng có thể xảy ra bất cứ lúc nào khi đã cấp kênh thoại cho MS cho nên một cuộc đàm thoại đã được kết nối có thể sẽ bị kiểm tra liên tục để tăng tính an toàn cho cuộc thoại đó.

Ta có thể đưa ra một số kết luận:

❖ *Hiệu lệnh chung*:

Được dùng với các CSDL cố định và hai CSDL bán cố định RAND và SSD-A nên đảm bảo được tính chống nhân bản vì các CSDL bán cố định thường xuyên được cập nhật. Nhưng ở đây cũng đặt ra hai vấn đề để đảm bảo tính an toàn đó là:

+ Phải đảm bảo giữ bí mật tuyệt đối đối với các cơ sở dữ liệu cố định dùng trong thuật toán gồm: ESN và MIN1, như các kỹ thuật đã nêu ở trên ta phải tăng cường khả năng bảo vệ, tránh được những kỹ thuật xâm nhập ngày càng cao, các cơ sở dữ liệu cố định phải có tính không thể đọc, dò bằng hiệu ứng điện, từ, hay bất cứ một phương pháp nào (có nghĩa là khi tiếp cận một module nhận dạng như UIM chẳng hạn, thì không thể dùng máy dò để có thể áp vào đó để đọc các giá trị ghi trong đó, vì hiện nay ngay cả máy tính các xung điện cũng có thể bị dò được và thông qua máy dò có thể tái hiện chính xác máy tính đó đang làm gì từ xa). Các CSDL phải được thiết kế sao cho nếu cố gắng phân tích (hay tháo ra) lập tức làm cho MS đó ngừng hoạt động.

  Giải pháp: Một trong các cách phòng chống là bằng cách dùng hộp khử điện từ để chống lại các xâm nhập bằng cảm ứng từ. Các chuẩn thì phải tuân theo nhưng công nghệ chế tạo mạch được giữ bí mật, ví dụ cách như bố trí ô nhớ, cấu trúc nhớ…

+ Vấn đề thứ hai là phải bảo vệ các dữ liệu truyền trong sóng vô tuyến như: RAND và SSD-A.

  Giải pháp: Chúng ta phải mật mã hoá các dữ liệu này trên đường truyền, bằng các phương thức mã hoá đã nêu ở trên như mã khối, mã đường, thay thế, mã RSA, mã DES… Vì đây là phần thuật toán hay phần mềm nên ta có thể không ngừng cải tiến và tìm các thuật toán mới để đảm bảo an toàn tuyệt đối cho các cơ sở dữ liệu này.

Ta có thể thấy rằng các cơ sở dữ liệu cố định là cái đầu tiên mà kẻ xâm nhập phải nghĩ đến khi thực hiện xâm nhập một máy cụ thể, nếu không biết được các mã số này thì họ chẳng làm được việc gì, vì đó đơn giản là một máy nào đó chứ không phải là máy họ cần xâm nhập. Giả sử người xâm nhập bằng một cách nào đó có thể dò được ESN tương ứng với MIN của MS đó, thì vấn đề còn lại sẽ là dò tìm các cơ sở dữ liệu bán cố định, nếu giải thuật mật mã hoá đưa ra tốt thì việc dò tìm mã khoá cho những giải thuật này không còn cách nào khác là phải dò tìm theo kiểu vét cạn, quá trình này đòi hỏi rất nhiều thời gian. Vấn đề là ta phải xây dựng một thuật toán có không gian khoá đủ lớn để với kỹ thuật hiện nay và các kỹ thuật trong tương lai (mà dựa vào công nghệ hiện nay có thể đoán được) có thể đạt được tốc độ xử lý nhanh bao nhiêu chăng nữa thì thời gian tiến hành thủ tục dò khoá mã theo phương thức vét cạn cũng phải chiếm thời gian lớn. Cần lưu ý rằng các dữ liệu này là hoàn toàn ngẫu nhiên, nói cách khác dữ liệu sau hoàn toàn không tương quan đến dữ liệu trước đó, nên việc dò tìm dữ liệu trước không hề liên hệ đến dò tìm dữ liệu sau, tức là với CSDL mới người xâm nhập phải dò lại từ đầu. Các thuật toán để hoàn thiện hơn các thuật toán mật mã hoá sẽ là một hướng nghiên cứu đầy hứa hẹn không chỉ hôm nay mà còn cả trong tương lai.

❖ *Hiệu lệnh riêng:*

Có thể xảy ra bất cứ lúc nào khi cuộc gọi đã được kết nối, hay nói cách khác là máy MS luôn bị chất vấn bất cứ lúc nào, quá trình này ngoài các thông số cố định như MIN2, ESN, và MIN1, MS còn sử dụng dữ liệu ngẫu nhiên RANDU thu được từ BS và dữ liệu SSD-A của bản thân nó. Thông thường nó được khởi xướng bởi MSC để đáp ứng lại một số sự kiện (sự cố đăng ký, và sau chuyển giao thành công là các trường hợp thường gặp). Hiệu lệnh này được sử dụng để kiểm tra MS về nhận dạng của nó. Ngoài các yêu cầu về tăng cường tính an toàn cho các cơ sở dữ liệu như trình bày trên. Chúng ta còn tuỳ theo mức độ bảo mật mà khách hàng yêu cầu và các hệ thống phục vụ cho các đối tượng khác nhau (ví dụ như chính phủ) ta có thể tăng cường độ an toàn cho một thuê bao khi chúng ta cho tăng cường mật độ hiệu lệnh riêng với thuê bao đó. Trong quá trình thực hiện hiệu lệnh riêng cũng tuỳ vào đối tượng ta có thể tiến hành hỏi lại một số lần, mức độ bảo mật càng cao thì số lần này càng ít, và nếu thấy khả nghi bị xâm nhập lập tức huỷ cuộc thoại đó, hay nói cách khác chúng ta có thể tiến hành "dịch vụ cung cấp độ bảo mật theo yêu cầu".

❖ *Cập nhật SSD*:

Ta thấy rằng chúng cũng có các yêu cầu về bảo đảm tính an toàn về các CSDL cố định và các CSDL bán cố định chuyển qua kênh vô tuyến. Trước hết phải giải được mã

để có RANDSSD, sau đó phải dùng các CSDL cần thiết A-key, ESN, và RANDSSD thu được để tiến hành thủ tục tạo SSD.

Nhận thấy rằng BS chỉ phát các số liệu ngẫu nhiên (RANDSSD) và số liệu kiểm tra AUTHBS đến MS đây cũng là một cách hạn chế tối đa về khả năng có được SSD mới của kẻ xâm nhập vì trước hết chúng phải giải mã được số liệu ngẫu nhiên RANDSSD, sau đó phải có các CSDL cố định thì mới có được SSD-NEW.

- ***Vấn đề MS chuyển mạng***

Chuyển mạng là khả năng cung cấp dịch vụ cho các MS ở ngoài vùng đăng ký thường trú của chúng. Khi MS chuyển mạng, đăng ký khởi xướng cuộc gọi và kết cuối cuộc gọi cần thêm các bước bổ sung. Mỗi khi lấy số liệu từ EIR mà số liệu này chưa có, EIR phải hỏi HLR chủ để cung cấp số liệu. Số liệu này bao gồm MIN, tóm tắt dịch vụ, các số liệu bí mật dùng chung (SSD) để nhận thực và các số liệu cần thiết khác để xử lý cuộc gọi. Thời gian thích hợp nhất để lấy các số liệu này lúc MS đăng ký với hệ thống, nơi mà nó đang có mặt.

Khi đã lưu giữ số liệu của MS chuyển mạng vào EIR, thì quá trình xử lý cuộc gọi và nhận thực sẽ giống với các dịch vụ của MS tại nơi thường trú. Tuy nhiên có thể xảy ra trường hợp mà MS khởi xướng cuộc gọi trước khi thực hiện đăng ký hay khi số liệu EIR chưa có. Khi này cần phải có thêm các bước bổ xung để EIR nhận số liệu từ HLR. Vậy mọi dịch vụ khởi xướng có hai bước tuỳ chọn trong đó EIR phát bản tin (sử dụng báo hiệu IS-41 của SS7) đến HLR để yêu cầu số liệu về MS chuyển mạng. HLR sẽ gửi bản tin với các thông tin tương ứng.

Khi MS bật nguồn nó phải đăng ký với hệ thống. Khi đăng ký, nó phát IMSI của mình và số liệu khác cho mạng. Khi này EIR ở hệ thống khách hỏi HLR của hệ thống chủ (hệ thống mà MS đăng ký dịch vụ) thông tin tóm tắt về dịch vụ (xem cho phép những dịch vụ gì đối với MS đó) và số liệu bảo mật. Sau đó EIR ấn định nhận dạng thuê bao di động tạm thời (TMSI_ chứa các thông tin cần thiết cho quá trình nhận thực) cho MS. MS sử dụng TMSI để truy nhập đến hệ thống. TMSI đảm bảo tính bảo mật thông tin vì chỉ MS và mạng biết nhận dạng MS thông qua TMSI. Khi MS chuyển vào một hệ mới, EIR của hệ mới sẽ thực hiện cấp một TMSI mới cho MS với các thông số từ EIR cũ. Trong đó các EIR phải thực hiện thủ tục nhận thực ấn định TMSI, trong thủ tục này các thông số đầu vào như trên bảng hình 5.6 và sơ đồ quá trình nhận thực ấn định TMSI được tiến hành như sơ đồ quá trình hiệu lệnh chung, nếu thành công MS được ấn định TMSI mới, nếu thất bại mạng sẽ khởi đầu hiệu lệnh duy nhất.

Mạng phát số ngẫu nhiên RAND cho tất cả MS. Khi MS truy nhập mạng, nó tính toán AUTHR với phiên bản mới nhất được mật mã hoá của RAND và sử dụng SSD-A. Sau đó phát bản tin cần thiết để nhận thực đến mạng. Mạng thực hiện tính toán tương tự và khẳng định nhận dạng MS. Tất cả các thông tin giữa BS và MS được mật mã để ngăn chặn kẻ khác giải mã số liệu và sử dụng số liệu này để nhân bản các MS khác. Ngoài ra mỗi khi MS khởi xướng hay kết thúc cuộc gọi, thông số đếm lịch sử cuộc gọi (COUNT) tăng thêm.

- ***Cập nhật thông số lịch sử cuộc gọi.***

Để ngăn chặn sự nhân bản, hệ thống WCDMA phải cập nhật thông số lịch sử cuộc gọi. Thủ tục này được thực hiện khi MSC cần hướng dẫn MS cập nhật lịch sử cuộc gọi (COUNT). Quá trình này được thực hiện ở thời điểm thuận tiện sớm nhất sau khi một kênh lưu lượng được ấn định cho khởi đầu cuộc gọi hoặc kết cuối cuộc gọi.

MSC phát bản tin yêu cầu cập nhật thông số (Parameter Update Request) đến BS. Khi thu được bản tin này, BS hướng dẫn MS cập nhật COUNT của nó bằng cách phát lệnh cập nhật thông số (Parameter Update Order). Khi thu được lệnh này, MS tăng đếm lịch sử cuộc gọi và lập tức gửi bản tin khẳng định cập nhật thông số (Parameter Update Confirm) đến MSC. Khi thu được bản tin này, MSC tăng đếm (COUNT) của nó. Như vậy là sau mỗi cuộc gọi COUNT của MS và COUNT tương ứng ở MSC chủ lại tăng nên 1, điều này giúp kiểm soát tốt hơn MS khi tiến hành so sánh 2 giá trị COUNT được lưu trữ ở hai nơi.

5.3. Bảo mật thoại

Có thể thấy rằng bản thân các mã định kênh và mã xáo trộn (long code và short code) trong WCDMA làm cho dữ liệu bị ngẫu nhiên hoá (hoặc giả ngẫu nhiên) nên các kênh truyền đã mang tính bảo mật. Tuy nhiên để tăng tính bảo mật cho các dữ liệu truyền trên kênh truyền nhằm chống lại các xâm nhập thụ động cũng như xâm nhập tích cực, hệ thống WCDMA còn có thể áp dụng các phương pháp mật mã hoá chẳng hạn như các phương pháp mã đường, thay thế bit, hay các thuật toán RSA, DES …và kết hợp với kiểm tra tính toàn vẹn của bản tin khi dùng thuật toán hàm Hash. Không thể yêu cầu bảo mật thoại nếu như quá trình xác thực chưa được thực hiện.

5.4. Các thuật toán tính toán số liệu nhận thực

Trong các thuật toán nhận thực dùng trong WCDMA ta quan tâm đến các thuật toán làm việc với dữ liệu dạng khối, mã hoá khối dữ liệu đối xứng (ví dụ như DES) và các hàm một chiều …

Bây giờ chúng ta xem xét một số thuật toán tạo ra dữ liệu nhận thực.

A. *Kỹ thuật tạo khoá (I) và tính toán AUTHR*

Kỹ thuật này được ứng dụng trong thuật toán hiệu lệnh chung

Giả sử M_1, M_2, M_3 là các dãy bit nhận được từ việc chia giá trị 172 bit thành các dãy 48 bit, 64 bit, và 64 bit tương ứng. Giá trị 172 bit là sự kết hợp 152 bit đầu vào (bao gồm RAND 32 bit, ESN 32 bit, MIN1 24 bit, và SSD-A 64 bit) với 24 bit 0 được thêm vào.

❖ *Tạo khoá*:

M_1 = 48 bit sẽ được sử dụng làm đầu vào của giai đoạn tạo khoá như sơ đồ thực hiện hình 5.15. Chúng ta sắp xếp 48 bit thành mảng 6 x 8 như hình 5.14

Quá trình này là bước thực hiện hoán vị 48 bit đầu vào

Ví dụ 1:

➢ Giả sử dãy dữ liệu M_1 là 16c27a415f39 (mã hexa) = 0001 0110 1100 0010 0111 1010 0100 0001 1111 0011 1001 (mã nhị phân)

Thực hiện hoán vị theo bảng 5.14 đối với M_1 ta được:

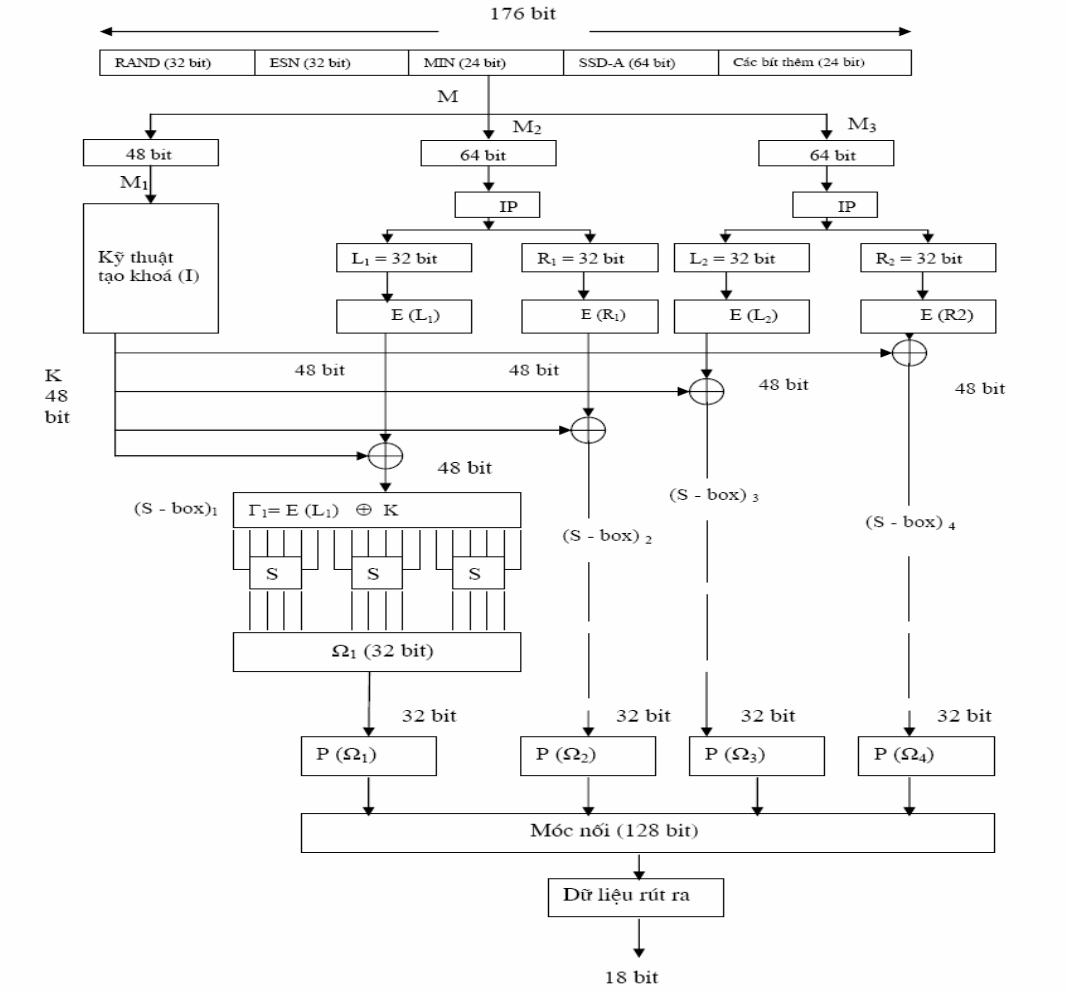
K = 0000 0001 1001 0101 1001 1101 0111 1000 0101 0111 1110 0100

(mã nhị phân) = 01959d7857e4 (mã hexa)

11	35	5	47	17	41	29	23
7	31	1	43	13	37	25	19
9	33	3	45	15	39	27	21
12	36	6	48	18	42	30	24
8	32	2	44	14	38	26	20
10	34	4	46	16	40	28	22

Hình 5.14: bảng sắp xếp các bit đầu vào của thuật toán tạo khoá

Ở đây 48 bit khoá K được tính bởi kỹ thuật tạo khoá (I) được biểu diễn trong hình 5.15



Hình 5.15: Tính toán AUTHR (18 bit) cho hiệu lệnh chung

❖ *Sử lý các khối*:

➢ Giả sử khối dữ liệu M_2 (64 bit) là 1 7 b 4 3 9 a 1 2 f 5 1 c 5 a 8.

- Thuật toán IP

Đầu tiên khối dữ liệu M_2 trước hết được đưa vào khối hoán vị ban đầu (IP) để chia thành hai khối L_1 (trái) và R_1 (phải), mỗi khối chứa 32 bit như được chỉ ra trong bảng trong hình 5.16

Thực hiện hoán vị bằng bảng IP, qua xáo trộn chuỗi ban đầu trở thành hai chuỗi con như sau:

L_1 (32 bit) = 6 0 2 7 5 3 7 d và R_1 (32 bit) = c a 9 e 9 4 1 1

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Hình 5.16. bảng hoán vị ban đầu (IP)

- Tác động của hàm E

Đến đây L_1 và R_1 được mở rộng thành 48 bit tương ứng với bảng sau:

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Hình 5.17. bảng thực hiện mở rộng

Trước hết xét L_1:

$E(L_1)$ là một hàm nhận 32 bit đầu vào và tạo ra 48 bit đầu ra, theo bản trên ta tính được: $E(L_1)$ = b 0 0 1 0 e a a 6 b f a

- Thực hiện cộng khoá K

Khi $E(L_1)$ đã được tính toán xong nó sẽ cộng tuyệt đối bit – bit với khoá K như sau:

Γ_1 (48 bit) = $E(L_1) \oplus K$ = (b19493d23c1e)

- Hoạt động của S-box

48 bit Γ_1 trở thành đầu vào của bộ thay thế không tuyến tính để tạo ra 32 bit ở đầu ra.

Véc tơ 48 bit Γ_1 trở thành thông số đầu vào cho $(S - box)_1$ từ S_1 đến S_8. Với mỗi S_i trong đó $1 \leq i \leq 8$ là các ma trận 4 hàng và 16 cột được biểu diễn trong bảng chuyển

đổi S_box ở hình 4.5. Đầu vào S_i là sự kết hợp 6 bit, trong đó bit đầu và bit thứ sáu là để hợp thành số chỉ hàng, còn 4 bit giữa để chỉ số cột trong bảng. Ví dụ đối với đầu vào là 010011 đến S_1, được chỉ ra là S_i^{01} (1001) , hàng 01 hay là hàng 1 và chỉ số cột là 1001 có nghĩa là cột 9.

Cấu tạo của bảng S_box đã được nêu trong chương 4 hình 4.5 phần thuật toán DES

Γ_1 (48 bit) = b 1 9 4 9 3 d 2 3 c 1 e trong hệ nhị phân là:

1011 0001 1001 0100 1001 0011 1101 0010 0011 1100 0001 1110

Nhóm thành các nhóm 6 bit là:

101100 011001 010010 010011 110100 100011 110000 011110

Dễ dàng tính được đầu ra dựa vào bảng S-box

$S_1^{10}(0110) = S_1^2(6) = 2 = 0010$

$S_2^{01}(1100) = S_2^1(12) = 6 = 0110$

$S_3^{00}(1001) = S_3^0(9) = d = 1101$

$S_4^{01}(1001) = S_4^1(9) = 7 = 0111$

$S_5^{10}(1010) = S_5^2(10) = c = 1100$

$S_6^{11}(0001) = S_6^3(1) = 3 = 0011$

$S_7^{10}(1000) = S_7^2(8) = a = 1010$

$S_8^{00}(1111) = S_8^0(15) = 7 = 0111$

Móc nối tất cả các số 4 bit này ta sẽ được một trường 32 bit Ω_1:

Ω_1 = 0010 0110 1101 0111 1100 0011 1010 0111 = 26d7c3a7

- Tác động của hàm P

Ω_1(32 bit) trở thành đầu vào của thuật toán P, thuật toán P hoán vị vị trí các bit trong Ω_1 theo bảng 5.18

Kết quả là đầu ra của phép hoán vị theo ma trận P:

$P(\Omega_1)$ = 1100 01 1 0110 0111 0011 1111 0011 0001 = c5673f31

Tiếp theo ta xét đến khối R_1(32 bit) .

- Sử dụng bảng mở rộng bit 5.17 ta có: $E(R_1)$ = e554fd4a80a3

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Hình 5.18. Ma trận P

- Cộng tuyệt đôi với khoá K tạo thành 48 bit

  Γ_2 = E(R_1) ⊕ K = e4c16032d747

- Chia thành 8 bộ 6 bit cho vào trường $(S\text{-box})_2$, xét tương tự như trên

  đầu ra của $(S\text{-box})_2$ sẽ là: Ω_2= a30abf88

- Tính P(Ω_2)

Sử dụng bảng hàm hoán vị P 5.18 ta được

P(Ω_2) = 79e06c9

Như vậy hai khối dữ liệu hoán vị P(Ω_1) và P(Ω_2) tương ứng với khối dữ liệu M_2 đã được tính toán.

➢ Giả sử rằng khối dữ liệu M_3 (64 bit) là 51cb36af3000000 .

Thực hiện tất cả các bước tương tự như trên:

- Sử dụng bảng hoán vị ban đầu chuỗi bit M_3 sẽ bị hoán vị thành 13050c1ba0c0a1e, trong đó L_2 = 13050c1b và R_2 = 0a0c0a1e.
- Cả L_2 (nửa bên trái) và R_2 (nửa bên phải) của M_3 đều được mở rộng từ 32 bit thành 48 bit dựa và bảng mở rộng bit phía trên, theo đó:

  E(L_2) = 8a680a8580f6

- Sau đó E(L_2) hoặc E(R_2) cộng trực tiếp với khoá K đã được tạo ra ở trên:

  Γ_3 = E(L_2) ⊕ K = (8bfd97fdd712)

- 48 bit này là đầu vào của $(S\text{-box})_3$. Hoạt động của $(S\text{-box})_3$ tương tự như trên

đầu ra của $(S\text{-box})_3$ như sau:

$$\Omega_3 = 19cc3369$$

- Sau đó Ω_3 hoán vị tạo ra 32 bit từ 32 bit đầu vào theo bảng hàm hoán vị P ta thu được kết quả:

$$P(\Omega_3) = 28397dc2$$

Cuối cùng đối với $R_2 = 0a0c0a1e$ là kết quả nhận được từ sự hoán vị ban đầu của M_3.

- Mở rộng : dựa vào bảng mở rộng bit phía trên ta có:

  $E(R_2) = 0540580540fc$

- Cộng tuyệt đối

$$\Gamma_4 = E(R_2) \oplus K$$
$$= 04d5c57d718$$

- Cho kết quả thu được vào bảng S ta thu được: $\Omega_4 = 08eb665$
- Hoán vị Ω_4 bằng ma trận P ta được: $P(\Omega_4) = 807d0dec$

Như vậy chúng ta đã tính được 4 dãy số riêng lẻ $P(\Omega_1)$, $P(\Omega_2)$, $P(\Omega_3)$ và $P(\Omega_4)$. Chúng ta tiến hành ghép 4 dãy số riêng lẻ này thành một dãy số duy nhất như sau:

$P(\Omega) = P(\Omega_1) \,||\, P(\Omega_2) \,||\, P(\Omega_3) \,||\, P(\Omega_4)$.

$P(\Omega) = (c5673f31) \,||\, (79e06c9) \,||\, (28397dc2) \,||\, (807d0dec)$

Cuối cùng 18 bit dữ liệu nhận thực được tính toán từ 128 bit trên bằng cách lấy bit thứ 7 của mỗi nhóm 7 bit

AUTHR = 011111000011000101.

Chương trình mô phỏng được biểu diễn trong đĩa CD kèm theo tài liệu.

B. ***Tính toán giá trị nhận thực sử dụng móc nối, hoán vị, và thay thế (S –box)***

Như mô tả dưới đây, thủ tục tính toán được thực hiện thứ tự như sau:

1. Mở rộng 152 bit thành 176 bit bằng cách cộng thêm 24 bit 0.
2. Chia 176 bit trên thành 3 khối: $M_1 = 48$ bit, $M_2 = 64$ bit, và $M_3 = 64$ bit. Sử dụng M_1 như một khoá 48 bit

3. Chia 48 bit của M_1 thành hai nửa : K_l = 24 bit và K_r = 24 bit
4. Thực hiện hoán vị ban đầu (IP) các khối M_2 và M_3 để trở thành L_0 và R_0 tương ứng, như vậy L_0 = 64 bit và R_0 = 64 bit
5. Thực hiện móc nối K_l với L_0 thành một khối 88 bit: $L_0 \| K_l$ = 88 bit
6. Thực hiện móc nối kết quả thu được từ phép móc nối trên với R_0 theo trật tự: $L_0 \| K_l \| R_0$ → 152 bit
7. Thực hiện móc nối kết quả thu được từ bước 6 với K_r giống như sau:

   $L_0 \| K_l \| R_0 \| K_r$ → 176 bit
8. Chia 176 bit thu được từ trên thành 4 phần:

   N_1 = 32 bit, N_2 = 48 bit, N_3 = 48 bit, N_4 = 48 bit
9. Mở rộng 2 bit N_1 thành $E(N_1)$ = 48 bit bằng cách sử dụng bảng mở rộng bit đã nêu ở trên.
10. Thực hiện biến đổi 4 khối trên qua S – box, kết quả tạo thành 4 khối 32 bit
11. Cho kết quả qua ma trận P thực hiện việc hoán vị các bit tạo ra 4 khối 32 bit
12. Kết quả của chúng được cộng modulo -2 với nhau để trở thành một đầu ra 32 bit.
13. Thực hiện cho 32 bit làm đầu vào của thuật toán hoán vị dùng ma trận P để có đầu ra là một khối 32 bit
14. Thực hiện mở rộng bằng ma trận mở rộng E tạo ra khối 48 bit
15. Cuối cùng 48 bit, bỏ 6 bit có trọng số cao nhất và 6 bit có trọng số nhỏ nhất và chọn (cứ hai bit thì lấy một bit) để trở thành AUTHR 18 bit.

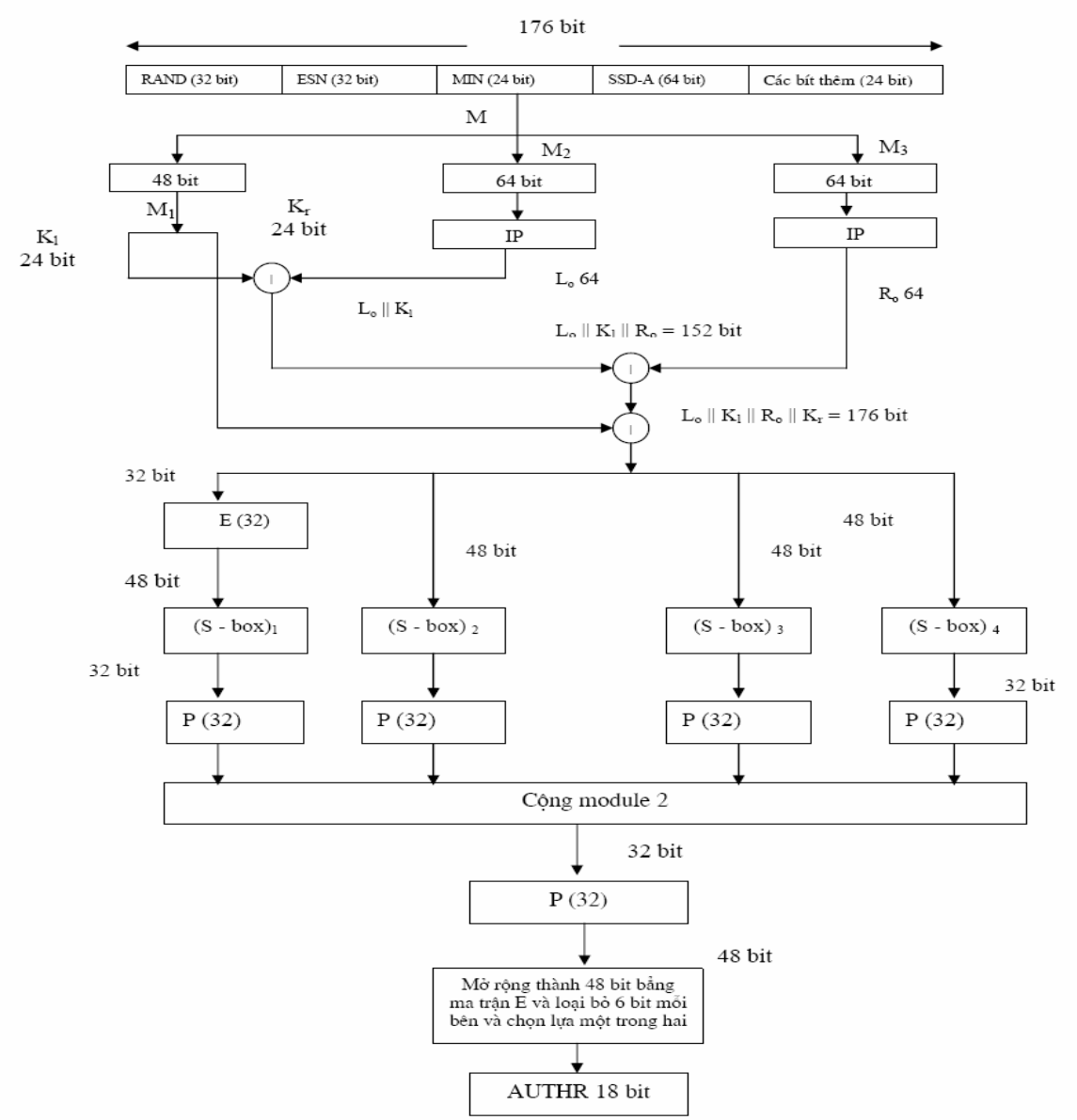
Chương trình thực hiện mô phỏng được trình bày trong phần phụ lục

Với ví dụ: Các khối đầu vào M_1 = 16c27a415f39, M_2 = 17b439a12f51c5a8, M_3 = 51cb36af43000000

Sau các bước thực hiện đã cho ta kết quả cuối cùng:

AUTHR = 110011101100000001

Chương trình này cho kết quả tính toán (với máy Pentium IV, tốc độ 1.3 Ghz) $execution\_time_{TB}$ = 0.2137 (s)



Hình 5.19.Sơ đồ thực hiện tính toán AUTHR với kỹ thuật móc nối, thay thế, và hoán vị

C. *Tính toán AUTHR sử dụng kỹ thuật DM*

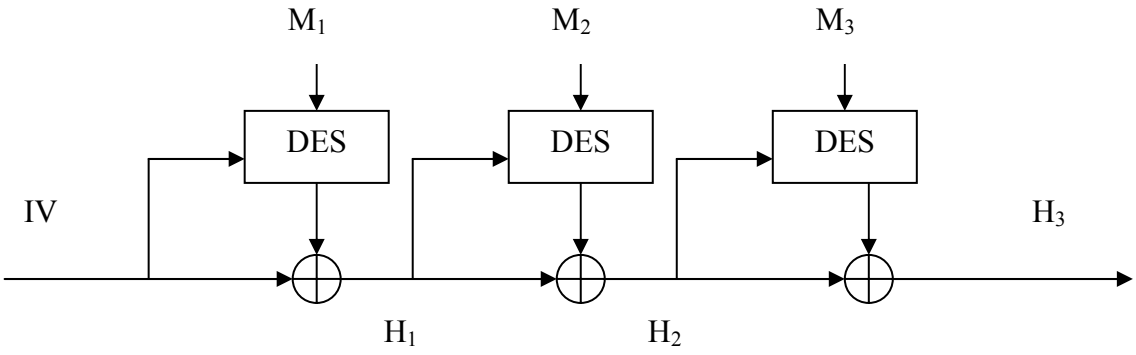
Kỹ thuật DM do Davies và Meyer đề xuất năm 1985, được ứng dụng để thực hiện tạo khoá trong kỹ thuật tạo số liệu nhận thực AUTHR, dựa trên ý tưởng của thuật toán CBC như đã nêu ở chương trước.

Trong kỹ thuật này sử dụng thuật toán DES trong quá trình tạo khoá theo sơ đồ sau:

Trong đó khối IV là khối khởi đầu bất kỳ, và để tăng tính ngẫu nhiên hoá, người ta thường thay đổi số liệu này.

Các bước thực hiện như sau:

1. Tạo ra 192 bit từ 152 bit các CSDL ban đầu của hiệu lệnh chung, bằng cách cộng thêm 40 bit 0 vào cuối
2. Chia khối 192 bit trên thành ba khối, mỗi khối 64 bit, các khối này sẽ dùng để tạo khoá bằng kỹ thuật DES như hình 5.20



Hình 5.20. Thuật toán tính toán số liệu nhận thực sử dụng kỹ thuật DM

3. Chọn một số khởi đầu ngẫu nhiên 64 bit IV (hoặc H_0), khối này sẽ đóng vai trò là dữ liệu đầu vào của thuật toán DES
4. Tính toán H_1 qua thuật toán DES với khoá lặp 16 lần như trong thuật toán DES (mỗi khối vòng lặp 16 lần rồi mới cho kết quả cuối cùng), và đầu ra H_1 là đầu vào của khối thứ hai
5. Thực hiện tính toán tương tự với khối thứ hai, đầu ra H_2 lại là đầu vào của khối thứ ba qua 16 vòng lặp
6. Thực hiện tính toán tương tự với khối cuối cùng – khối thứ ba, kết quả chúng ta thu được một khoá H_3 64 bit để từ đó tạo nên AUTHR
7. loại 5 bit có trọng số cao nhất và 5 bit có trọng số thấp nhất, còn 54 bit, lấy một bit trên mỗi tập hợp ba bit chúng ta có được 18 bit AUTHR

Các bước thực hiện thuật toán DES đã được diễn tả rõ ràng ở chương trước

Sau khi thực hiện mô phỏng bằng phần mềm (có thể tham khảo trong CD) và thực hiện với:

Ví dụ: các khối đầu vào M_1= 7a138b2524af17c3, M_2 = 17b439a12f51c5a8, M3 = 51cb360000000000, H_0(IV) = 67542301efcdab89

Kết quả thu được: AUTHR = 100001110101111110

Chương trình này thực hiện với thời gian thực hiện: $execution\_time_{TB} = 3.484$ (s)

D. ***Chương trình cập nhật SSD bằng thuật toán MD5***

Quy trình này sử dụng thuật toán băm một chiều MD5 như đã nêu ở phần trước.

Trong đó sử dụng các hàm cơ sở: F, G, H, I

$$F(X, Y, Z) = X.Y + X'.Z$$

$$G(X, Y, Z) = X.Z + Y.Z'$$

$$H(X, Y, Z) = X \oplus Y \oplus Z$$

$$I(X, Y, Z) = Y \oplus (X + Z')$$

Trong đó X' = Not (X).

Đây là các hàm không tuyên tính thực hiện tham chiếu theo hình sau:

X	Y	Z	F	G	H	I
0	0	0	0	0	0	0
0	0	1	1	0	1	0
0	1	0	0	1	1	0
0	1	1	1	0	0	1
1	0	0	0	0	1	1
1	0	1	0	1	0	1
1	1	0	1	1	0	0
1	1	1	1	1	1	0

Hình 5.21: Bảng tham chiếu các hàm cơ bản F, G, H, I của thuật toán tạo khoá

Quá trình cập nhật SSD được thực hiện theo các bước sau đây:

1. Từ các bit ban đầu cộng thêm để tạo nên một khối 512 bit, chia khối này thành 16 khối M[i], $0 \le i \le 15$
2. Đặt các giá trị khởi đầu cho thuật toán MD5 A = 67452301, B = EFCDAB89, C = 98BADCFE, D = 10325476
3. Tác dụng của các hàm F, G, H, I đối với các khối trên, trong đó các hàm được định nghĩa như sau:

   FF (a, b, c, d, M[k], s, i): a =b + ((a + F (b, c, d) + M[k] +T[i]) <<< s)

GG (a, b, c, d, M[k], s, i): a =b + ((a + G (b, c, d) + M[k] +T[i]) <<< s)

HH (a, b, c, d, M[k], s, i): a =b + ((a + H (b, c, d) + M[k] +T[i]) <<< s)

II (a, b, c, d, M[k], s, i): a =b + ((a + I (b, c, d) + M[k] +T[i]) <<< s)

s là số bước dịch trái.

i là chỉ số của phần tử mảng T, với thứ tự như sau : từ trên xuống dưới và từ trái sang phải

D76AA478	F61E2562	FFFA3942	74B1A24D
E8C7B756	C0414BC0	8771F681	43AB0398
242070DB	265E5A51	069D9122	AB9427E9
C1BDCEEE	E9B6C7AA	FDE5380C	3D93A27B
F57C0FAF	D62F105D	1D1652A6	665B99C3
3AAB1B7B	02441453	0276AEC0	8F2CCC92
20BCA6E1	D8A1E681	7472BD08	0010147D
DD529708	E7D3FBC8	38683A08	85A465D1
43476BAB	21E1CDE6	A324F8AE	77A8864F
55EFE87C	C33707D6	EAA127FA	862CEEE0
FFFF5BB1	F4D50D87	DAEF3085	2301E396
895CD7BE	455A14ED	0488B585	CF281DA3
6B901122	A9E3E905	D9D568B9	F883908B
FD987193	FCEFA3F8	E6DB99E5	DD5F0235
A679438E	676F02D9	1FA27CF8	2ADCE2DB
49B40821	8D2A4C8A	C4AC5665	EB87D391

Hình 5.22. Ma trận T

Thực hiện tính toán 4 vòng, 64 bước theo thứ tự sau đây:

- Vòng 1: Tính toán FF (a, b, c, d, M[k], s, i)

  hay tính toán: a =b + ((a + F (b, c, d) + M[k] +T[i]) <<< s)

FF(A,B,C,D,M0,7,1);	FF(D,A,B,C,M1,12,2);	FF(C,D,A,B,M2,17,3);	FF(B,C,D,A,M3,22,4);
FF(A,B,C,D,M4,7,5);	FF(D,A,B,C,M5,12,6);	FF(C,D,A,B,M6,17,7) ;	FF(B,C,D,A,M7,22,8);
FF(A,B,C,D,M8,7,9);	FF(D,A,B,C,M9,12,10);	FF(C,D,A,B,M10,17,11);	FF(B,C,D,A,M11,22,12);

FF(A,B,C,D,M12,7,13); FF(D,A,B,C,M13,12,14); FF(C,D,A,B,M14,17,15); FF(B,C,D,A,M15 ,22,16);

- Vòng 2:Tính GG (a, b, c, d, M[k], s, i) hay

a =b + ((a + G (b, c, d) + M[k] +T[i]) <<< s)

GG(A,B,C,D,M1,5,17); GG(D,A,B,C,M6,9,18); GG(C,D,A,B,M11,14,19); GG(B,C,D,A,M0,20,20);

GG(A,B,C,D,M5,5,21); GG(D,A,B,C,M10,9,22); GG(C,D,A,B,M15,14,23); GG(B,C,D,A,M4,20,24);

GG(A,B,C,D,M9,5,25); GG(D,A,B,C,M14,9,26); GG(C,D,A,B,M3,14,27); GG(B,C,D,A,M8,20,28);

GG(A,B,C,D,M13,5,29); GG(D,A,B,C,M2,9,30); GG(C,D,A,B,M7,14,31); GG(B,C,D,A,M12,20,32);

- Vòng 3: Tính HH (a, b, c, d, M[k], s, i) hay

a =b + ((a + H (b, c, d) + M[k] +T[i]) <<< s)

HH(A,B,C,D,M5,4,33); HH(D,A,B,C,M8,11,34); HH(C,D,A,B,M11,16,35); HH(B,C,D,A,M14,23,36);

HH(A,B,C,D,M1,4,37); HH(D,A,B,C,M4,11,38); HH(C,D,A,B,M7,16,39); HH(B,C,D,A,M10,23,40);

HH(A,B,C,D,M13,4,41); HH(D,A,B,C,M0,11,42); HH(C,D,A,B,M3,16,43); HH(B,C,D,A,M6,23,44);

HH(A,B,C,D,M9,4,45); HH(D,A,B,C,M12,11,46); HH(C,D,A,B,M15,16,47); HH(B,C,D,A,M2,23,48);

- Vòng 4: Tính II (a, b, c, d, M[k], s, i) hay

a =b + ((a + I (b, c, d) + M[k] +T[i]) <<< s)

II(A,B,C,D,M0,6,49); II(D,A,B,C,M7,10,50); II(C,D,A,B,M14,15,51); II(B,C,D,A,M5,21,52);

II(A,B,C,D,M12,6,53); II(D,A,B,C,M3,10,54); II(C,D,A,B,M10,15,55); II(B,C,D,A,M1,21,56);

II(A,B,C,D,M8,6,57); II(D,A,B,C,M15,10,58); II(C,D,A,B,M6,15,59); II(B,C,D,A,M13,21,60);

II(A,B,C,D,M4,6,61); II(D,A,B,C,M11,10,62); II(C,D,A,B,M2,15,63); II(B,C,D,A,M9,21,64);

4. Cuối cùng kết quả thu được là các biến a, b, c, d được đem cộng với các giá trị A, B, C, D ban đầu, và kết quả:

SSD-A = (a ⊕ A) || (b ⊕ B) và SSD-B = (c ⊕ C) || (d ⊕ D)

Sau khi thực hiện mô phỏng chương trình này (có thể tham khảo trong đĩa CD) và thực hiện với

Ví dụ:

Quá trình cập nhật với CSDL ban đầu: 7a138b2524af17c317b439a12f51c5a851cb36

Qua quá trình chương trình mô phỏng thực hiện cho ta kết quả

SSD_A_NEW = FD17A5E0BD2BA094

SSD_B_NEW = FC675723BE9C61B9

Thời gian thực hiện chương trình: execution_time = 2.6613 (s)

Ngoài các phương pháp trên ra còn rất nhiều các phương pháp để tạo ra dữ liệu nhận thực AUTHR và cập nhật SSD (*tham khảo thêm các chương trình mô phỏng với đĩa CD đi cùng tài liệu này*)

Nhận xét các thuật toán:

Đối với các thuật toán xử lý theo khối như kỹ thuật A và B, có thể xử lý các khối này một cách đồng thời thay vì xử lý tuần tự các khối như trên đã thực hiện, đây là điều kiện quan trọng để thực hiện việc xử lý song song. Các Chip xử lý cũng có thể dựa vào điều kiện này để thực hiện tính toán theo cấu trúc xử lý song song nhằm làm tăng tốc độ xử lý thuật toán.

Đối với các thuật toán đòi hỏi phải xử lý tuần tự như kỹ thuật DM và MD5 thì cách duy nhất để tăng tốc độ thực hiện thuật toán là tăng tốc độ xử lý tính toán từng bước.

Tuy nhiên dù là các thuật toán có thể sử lý song song hay các bước tuần tự thì khả năng bị giải mã không phải nằm ở bản thân thuật toán mà nằm ở các thông số mật đầu vào của thuật toán, do đó vấn đề mấu chốt là phải đảm bảo an toàn tuyệt đối cho các CSDL này. Với các thuật toán có các số liệu khởi đầu IV (khối dữ liệu khởi đầu của bản thân thuật toán) ta có thể tăng độ an toàn bằng cách thường xuyên thay đổi các số liệu này.

Kết luận:

Qua quá trình thực hiện mô phỏng các thuật toán, tôi nhận thấy rằng:

- Việc sử dụng các thuật toán này vào thủ tục nhận thực và bảo mật thông tin trong hệ thống WCDMA là phù hợp.
- Các chương trình thử cũng sẽ phải thực hiện các bước lần lượt như trên, thời gian thực hiện các chương trình tương đối lớn (nhanh: 0.2 (s), chậm đến hơn 3(s)), tất nhiên đây mới chỉ thử trên máy PC, không phải là máy chuyên dụng. Trên thực tế các quá trình này sẽ được thực hiện trên các Chip chuyên dụng đạt tốc độ nhanh hơn, tuy nhiên với số lượng các bước và với tốc độ xử lý hiện nay và trong một tương lai gần, các khoá cũng có thể bị phá nhưng việc này chiếm một thời gian đủ lớn để ta có thể khẳng định đó là thuật toán an toàn

- Trong các kỹ thuật nêu trên, quan trọng nhất là các CSDL cố định và bán cố định phải được đảm bảo an toàn tuyệt đối. Vấn đề mấu chốt của chúng ta là phải có các thuật toán mật mã hoá hoàn thiện, do đó các thuật toán phục vụ cho mục đích này luôn cần được cải tiến, hoàn chỉnh để có thể thực hiện truyền các CSDL bán cố định một cách an toàn. Chúng ta cần phải nghiên cứu các thuật toán hoàn chỉnh hơn theo kiểu hàm một chiều (hay hàm một phía) có không gian khoá nhiều hơn, mang tính ngẫu nhiên hoá cao để có thể chống lại các loại xâm nhập cả thụ động và tích cực.
- Song song với phát triển các kỹ thuật mật mã hoá, chúng ta còn phải nghiên cứu hoàn thiện các kỹ thuật lưu giữ các CSDL trước hết là đối với các CSDL cố định, sau đó đến các CSDL bán cố định, vì kỹ thuật lưu trữ càng tốt càng đảm bảo tính không thể xâm nhập của các dữ liệu này.
- Tăng cường nghiên cứu các thuật toán mang tính móc xích, như ta đã thấy chỉ có các thuật toán đòi hỏi kết quả tính toán sau liên quan chặt chẽ đến các kết quả tính toán trước đó thì mới có thể hạn chế được khả năng áp dụng cách sử lý song song - là một trong các cách làm tăng tốc độ thám mã.
- Đối với các CSDL bán cố định như SSD và COUNT, không cần phải chỉ khi đăng nhập hay kết cuối mới có sự cập nhật, trong một hệ thống cần các CSDL mang tính ngẫu nhiên cao, việc cập nhật các thông số này cần được xảy ra ở thời điểm bất kỳ. Đối với CSDL tăng từng bước một như COUNT, nên đưa vào các báo hiệu giả, tức là có báo hiệu như báo hiệu cập nhật nhưng thực ra không cập nhật thông số, tất nhiên đây cũng chỉ là ý tưởng, nhưng đôi khi chúng ta cũng áp dụng chiến thuật này để có thể lừa kẻ thám mã.

Với sự ứng dụng các thuật toán mật mã hiện đại một cách hiệu quả, hệ thống WCDMA đã có một cơ chế nhận thực tương đối hoàn chỉnh. Với các kỹ thuật mật mã hoá và bản thân kỹ thuật trải phổ đã làm cho WCDMA nhận được một sự đánh giá cao về khả năng bảo mật. Có thể nói rằng hệ thống WCDMA đã kế thừa tất cả các thành tựu của hệ thống di động thế hệ 2 (2G) để tạo nên một thế hệ viễn thông mới hoàn thiện hơn. Ở Việt Nam, bên cạnh việc tích cực nắm bắt, triển khai và ứng dụng các kỹ thuật viễn thông mới, ta có thể nghiên cứu cải tiến các thuật toán, và tạo ra các thuật toán mới thực sự hoàn thiện để góp phần phát triển kỹ thuật bảo mật ở các thế hệ di động và các thế hệ mạng viễn thông nói chung trong tương lai. Với tiềm năng con người của chúng ta, theo ý kiến tôi đây cũng chỉ là một sự phát huy tri thức và khả năng tính toán có sẵn trong mỗi chúng ta và tôi tin rằng điều đó là có thể thực hiện được.

TÀI LIỆU THAM KHẢO

[1] GS.TSKH. Phan Đình Diệu
Lý thuyết mật mã và An toàn thông tin (trang 8 -131)
Đại học công nghệ - Đại học quốc gia hà nội - 2002

[2] TS. Nguyễn Phạm Anh Dũng
CdmaOne và cdma2000 (trang 232 – 344) - Nhà xuất bản Bưu điện 2003

[3] TS. Nguyễn Phạm Anh Dũng
Thông tin di động thế hệ 3 (trang 191 - 202) - Nhà xuất bản Bưu điện 12-2001

[4] Trịnh Nhật Tiến
Một số vấn đề về an toàn dữ liệu (trang 3 – 37)
Đại học Công nghệ - Đại học Quốc gia Hà Nội

[5] PGS.TS. Thái Hồng Nhị & TS. Phạm Minh Việt
An toàn thông tin - Mạng máy tính truyền tin số và truyền dữ liệu (Trang 5 – 134)
Nhà xuất bản Khoa Học và Kỹ thuật 2004

[6] TS. Trịnh Anh Vũ
Giáo trình thông tin di động (chương 5 trang 38 - 48)
Đại học Công nghệ - Đại học Quốc gia Hà Nội

[7] Dr. Man Young Rhee
CDMA Cellular Mobile Communications and Network Security
Hanyang University, 1998 Prentice Hall PTR (Pages 355 – 507)

[8] J.S. Blogh, L. Hanzo
Third-Generation Systems and Intelligent Wireless Networking
2002 John Wiley & Sons Ltd (Pages 27 – 87)

[9] John.G van Bosese
Signaling in Telecommunication Network - 1998 John Wiley & Sons, Inc
(Chapter 17, pages 418 – 531)

[10] Keiji Tachikawa
W-CDMA: Mobile Communications System.
2002 John Wiley & Sons, Ltd (Pages 81 - 211)

[11] Nachiketh R.Potlapally Srivaths Ravi Amand Raghunathan
Optimizing Public-Key encryption for Wireless Clients
0 - 7803 – 7400 -2/02 (C) 2002 IEEE

[12] P. Nicopolitidis, M. S. Obaidat, G.I. Papadimitriou and A .S .Pornportsi
Wireless Networks 2003 John Wiley & Sons, Ltd. (Chapter 5, pages 151 - 188)

[13] Roger J. Sutton
Secure Communications. - 2003 John Wiley & Sons, Ltd.
(Pages 1 – 83 and 113 – 139)

[14] Raymond Steele, Chin-Chun Lee and Peter Gould
GSM, cdmaOne and 3G Systems - 2001 John Wiley & Sons Ltd
(Chapter 6, pages 404 - 498)

[15] Savo G. Glisic
Adaptive WCDMA: Theory and Practice.
2003 John Wiley & Sons, Ltd (Pages 519 – 537)

[16] Willie W. Lu SIEMENS, USA
Broadband Wireless Mobile: 3G and Beyond
2002- John Wiley & Sons, Ltd.ISBN: 0-471-48661-2 (Pages 215 – 220)