HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

ĐÀO ÁNH HƯƠNG

NGHIÊN CỨU PHƯƠNG PHÁP BẢO MẬT TIN NHẮN TRÊN ĐIỆN THOẠI DI ĐỘNG

Chuyên ngành: Hệ thống thông tin

Mã số: 60.48.01.04

Người hướng dẫn khoa học: TS NGUYỄN NGỌC CƯƠNG

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI – 2013

LỜI MỞ ĐẦU

Ngày nay, hệ thống mạng di động đã trở nên rất phổ biến trong xã hội, hầu hết mọi người đều sử dụng điện thoại di động. Cùng với sự phát triển đó, bên cạnh những tính năng ưu việt, các điện thoại di động rất dễ bị đánh cắp hoặc mất mát thông tin, đặc biệt là thông tin được trao đổi qua tin nhắn SMS. Nhưng hiện nay, việc trao đổi thông tin qua tin nhắn lại đang được nhiều người và nhiều lĩnh vực áp dụng như là: thương mại điện tử, Internet banking, liên lạc trao đổi giữa các thuê bao di động…

Bên cạnh đó, hiện nay có rất nhiều kẻ xấu lợi dụng những lỗ hổng trong quá trình truyền tin nhắn SMS để có kiếm tiền hoặc phục vụ mục đích xấu.

Việc nghiên cứu bảo mật thông tin điện thoại di động là một đề tài hấp dẫn và có ứng dụng thực tế cao, đang là chủ đề quan tâm nghiên cứu và phát triển ứng dụng mạnh mẽ hiện nay. Đó là lý tôi chọn đề tài: ***"Nghiên cứu phương pháp bảo mật tin nhắn trên điện thoại di động"*** làm đề tài luận văn tốt nghiệp của mình.

Cấu trúc của luận văn như sau:

LỜI CAM ĐOAN

MỤC LỤC

DANH MỤC CÁC CHỮ VIẾT TẮT

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH

LỜI MỞ ĐẦU

Chương 1: TỔNG QUAN VỀ BẢO MẬT TIN NHẮN TRÊN ĐTDĐ

1.1. Giới thiệu về dịch vụ tin nhắn SMS

1.2. Bảo mật tin nhắn trên ĐTDĐ

1.3. Giải pháp kỹ thuật để bảo mật tin nhắn

Chương 2: ỨNG DỤNG MÃ HÓA TRONG BẢO MẬT TIN NHẮN

2.1. Ứng dụng thuật toán AES trong bảo mật tin nhắn

2.2. Ứng dụng mật mã dựa trên định danh trong bảo mật tin nhắn

2.3. Một số thuật toán mã hóa khác ứng dụng trong bảo mật tin nhắn

Chương 3: XÂY DỰNG CHƯƠNG TRÌNH BẢO MẬT TIN NHẮN TRÊN ĐTDĐ

3.1. Xây dựng chương trình bảo mật tin nhắn trên ĐTDĐ

3.2. Thử nghiệm demo chương trình bảo mật tin nhắn trên ĐTDĐ

KẾT LUẬN

TÀI LIỆU THAM KHẢO

CHƯƠNG 1: TỔNG QUAN VỀ BẢO MẬT TIN NHẮN TRÊN ĐIỆN THOẠI DI ĐỘNG

1.1. Giới thiệu về dịch vụ tin nhắn SMS

1.1.1. ĐTDĐ và mạng thông tin di động

1.1.1.1. Mobile Phone Family

1.1.1.2. The flexible Mobile Phone

1.1.2. Short Message Service (SMS)

1.1.2.1. SMS là gì?

1.1.2.2. Lịch sử phát triển của SMS

1.1.3. Cách truyền và nhận tin nhắn SMS

Có hai trường hợp truyền và nhận tin nhắn SMS giữa các thuê bao di động: truyền nội bộ và truyền ra bên ngoài

1.2. Bảo mật tin nhắn trên ĐTDĐ

1.2.1.Tổng quan về bảo mật tin nhắn

Qua nhiều năm những ứng dụng của ĐTDĐ đang ngày càng tăng nhanh, đặc biệt, trong suốt thập kỷ vừa qua. Dịch vụ tin nhắn ngắn SMS là một trong những dịch vụ của ĐTDĐ có tính ứng dụng cao trong đời sống. Dịch vụ tin nhắn ngắn SMS đóng một vai trò quan trọng trong nhiều lĩnh vực như: thương mại điện tử, ngân hàng di động, ứng dụng dành cho chính phủ, và thông tin thường ngày. Bởi lẽ SMS là một dịch vụ không dây xuyên quốc gia, nó tạo điều kiện cho người dùng có thể liên lạc với bất kỳ số điện thoại nào trên thế giới ngay lập tức và không gặp bất cứ rắc rối nào.

Mục đích chính của SMS là phân phối tin nhắn từ điện thoại này đến điện thoại khác. Nó cung cấp nhiều lợi ích cho cuộc sống thường ngày của chúng ta. Tuy nhiên, dịch vụ SMS này chưa chắc đã an toàn và đảm bảo giữ bí mật những thông tin nhạy cảm. Nhiều nguy cơ từ dịch vụ SMS có thể phát sinh. Do đó việc ngăn chặn việc nội dung SMS bị chặn bất hợp pháp hoặc bị làm gián đoạn cũng như việc đảm bảo nguồn gốc của những tin nhắn là hợp pháp đóng vai trò rất quan trọng.

Một trong những thách thức quan trọng trong nền công nghiệp thông tin di động là đảm bảo cho dịch vụ di dộng được sử dụng đúng cách và không bị lạm dụng. Thêm nữa, nội dung SMS không được mã hóa trong suốt quá trình truyền cho phép các nhân viên tổng đài điện thoại đọc được và thay đổi nội dung đó. Mặt khác, dịch vụ SMS lại không có các thủ tục

có sẵn để rà soát hoặc cung cấp chế độ bảo mật cho dữ liệu hoặc văn bản được truyền đi. Rõ ràng là các phần của ứng dụng SMS cho thiết bị di động được thiết kế và phát triển mà không tính đến khía cạnh bảo mật SMS. Vì thế, tất cả những cơ sở vật chất của SMS nên kết hợp với một vài kỹ thuật bảo mật cơ bản để tăng cường tính bảo mật, tính toàn vẹn, xác thực và chống chối bỏ của tin nhắn trước khi chúng được sử dụng.

Trao đổi tin nhắn thông thường không đảm bảo tính bảo mật vì các tin nhắn được truyền đi trong chế độ văn bản (có thể đọc được) thông qua một kênh truyền không an toàn. Do tính chất đặc biệt của truyền thông di động và tính an toàn kém của kênh truyền, vấn đề an ninh an toàn đã trở thành một vấn đề được ưu tiên cao. Bên cạnh việc cải thiện và nâng cao tính bí mật của nội dung tin nhắn SMS, cũng cần phải đảm bảo mọi thứ đều hợp pháp. Mặt khác, các kênh truyền thông không được bảo vệ, các thiết bị không dây thì ngày càng phổ biến đã gây ra nhiều lỗ hổng bảo mật nghiêm trọng. Vì vậy, điều quan trọng là phải phát triển ứng dụng ĐTDĐ sao cho có thể đảm bảo danh tính chính xác của các bên giao tiếp, trong khi đó cũng cần đảm bảo tính bảo mật nội dung và tính toàn vẹn của tin nhắn SMS trong thời gian truyền dữ liệu để tránh những mối hiểm họa.

Mạng GSM không thể cung cấp nhiều dịch vụ bảo mật quan trọng cùng một lúc. Vì thế, quá trình truyền nội dung tin nhắn SMS sẽ xảy ra một số nguy cơ về bảo mật. Do đó, nhiều tiêu chuẩn mã hóa đã được các nhà cung cấp dịch vụ sử dụng để đảm bảo tính toàn vẹn và bảo mật trong quá trình truyền nội dung SMS. An ninh an toàn trong ngành viễn thông là điều vô cùng quan trọng. Hơn nữa, sự toàn vẹn và bảo mật có thể đạt được bằng cách mã hóa các phương tiện, và tính xác thực có thể thực hiện được bằng cách cài đặt một máy chủ phụ trợ được kết nối với các trung tâm tin nhắn SMSC.

Mặc dù mạng GSM đã áp dụng các kỹ thuật bảo mật khác nhau nhưng do tính mở của mạng không dây làm cho thông tin của các bên giao tiếp dễ bị gián đoạn hoặc bị chặn bởi những kẻ tấn công. Phương tiện truyền tải nội dung tin nhắn SMS cũng không hoàn toàn an toàn và dễ bị những kẻ tấn công theo dõi và gửi thông tin sai lệch, do đó mạng GSM có nhiều điểm yếu bảo mật khác nhau. Điều này cho phép những kẻ tấn công sử dụng những công cụ và cơ chế để đọc và sửa đổi những thông tin được gửi đi. Hơn nữa, có thể kiểu tấn công man in the middle (MITM) trong suốt quá trình xác thực cho phép kẻ tấn công lựa chọn một thiết bị di động của nạn nhân hoặc chính trạm xác thực tới một trạm giả mạo, nơi lần lượt chuyển tiếp lưu lượng truy cập xác thực tới mạng thực, dẫn đến việc mạo nhận trạm di động của nạn

nhân tới mạng thực và ngược lại. Rõ ràng là tồn tại rất nhiều rủi ro liên quan đến bảo mật trong suốt các thao tác truyền và phát SMS.

1.2.2. Phân tích những lỗ hổng bảo mật

Tin nhắn SMS có thể được truyền qua mạng di động GSM, GPRS, UMTS, CDMA. Ở đây, luận văn chỉ nghiên cứu lỗ hổng bảo mật của mạng GSM.

Khi nói về bảo mật thông tin, mọi người thường hay nói tới bảo mật mạng, bảo mật ứng dụng, bảo mật web. Sở dĩ ít có sự quan tâm đến lĩnh vực bảo mật mạng di động vì số lượng tấn công dựa trên điểm yếu của mạng di động chưa phổ biến và khó phát hiện. Tuy nhiên với sự bùng nổ của các thiết bị điện thoại thông minh, đi kèm với các lỗ hổng bảo mật trên môi trường di động ngày càng gia tăng, bảo mật mạng di động đang trở thành một chủ đề nóng. Hiện nay môi trường mạng di động đang được khai thác triệt để cho các ứng dụng cung cấp giá trị gia tăng dựa trên SMS, dịch vụ cung cấp thông tin trực tuyến, thậm chí cả dịch vụ rất nhạy cảm về an toàn thông tin là thanh toán trực tuyến bằng ĐTDĐ. Những dịch vụ này dựa trên các phương thức truyền dẫn cơ bản do mạng di động không dây cung cấp và những lỗ hổng bảo mật trên tầng không dây di động đều liên quan đến các dịch vụ trên.

1.2.2.1. Những lỗ hổng bảo mật trên mạng GSM

Trong việc đảm bảo không tiết lộ dữ liệu, GSM sử dụng thuật toán A5, tuy nhiên người ta đã chứng minh rằng thuật toán này yếu và có người có thể phân tích và tìm ra khóa bí mật trong vài phút. Hiện tại đã có những phiên bản tốt hơn của thuật toán nhưng nó vẫn không thể chống đỡ được với các cuộc tấn công của hacker.

ESMEs (External Short Messaging Entities) giao tiếp với SMSC được thực hiện thông qua giao thức Short Message Peer to Peer (SMPP). Các giao thức SMPP không mã hóa nội dung của SMS làm cho các SMS có nguồn gốc thông qua ESMEs dễ bị tấn công bởi phương thức man-in-the-middle. Bên cạnh việc mạng GSM sử dụng những thuật toán mã hóa yếu, mạng cũng không cung cấp dịch vụ bảo mật end-to-end. Điều này cho thấy cơ sở hạ tầng của mạng GSM tồn tại một số khu vực dễ dàng bị tấn công bởi phương thức man-in-the-middle.

Các cuộc tấn công lại có thể xảy ra với cơ chế xác thực trong hoạt động của mạng GSM. Cơ sở hạ tầng của GSM thiếu việc tự xác thực. Kết quả là việc mạo danh và giao dịch sai có thể được thực hiện từ đó ảnh hưởng đến cơ chế xác thực hiện tại.

Mặt khác, mạng GSM bảo mật bằng tính bất khả định có nghĩa là bảo mật bằng cách giấu kín thuật toán, cách thi hành, không cho cộng đồng biết được cơ chế bảo mật. Trong cơ chế bảo mật GSM, các thuật toán A3, A5, A8 đều được giấu kín. Tuy nhiên, quan điểm hiện

tại về an toàn thông tin cho rằng phương thức bảo mật bằng tính bất khả định này sẽ không an toàn. Lý do là một thuật toán cho dù tốt đến đâu cũng có thể mắc lỗi, và nếu không được công khai để cộng đồng kiểm chứng thì hoàn toàn có thể bị mắc những lỗi nghiêm trọng mà chưa ai biết. Thực tế đã chứng minh là dù được nhà sản xuất cố gắng giữ bí mật sau nhiều năm, hacker đã tìm được thông tin khá đầy đủ về các thuật toán A3, A5 và A8.

Hơn nữa, thuật toán A5 được dùng để mã hóa đường truyền sóng radio thoại và dữ liệu. Tuy nhiên có 3 chính sách mã hóa khác nhau: A5/0 (không mã hóa) và hai thuật toán A5/1 và A5/2. Sở dĩ có sự phân loại này là do các pháp chế về vấn đề xuất khẩu thuật toán bảo mật. Ba chính sách mã hóa A5 được phân loại như sau:

- Thuật toán A5/1 được sử dụng bởi những quốc gia là thành viên của tổ chức Viễn thông châu Âu CEPT, Mỹ, một số nước châu Á.

- Thuật toán A5/2 được sử dụng ở Úc, châu Á và một số nước thế giới thứ 3. Thuật toán A5/2 ra đời sau, yếu hơn thuật toán A5/1 và chủ yếu được sử dụng cho mục đích xuất khẩu sang các nước nằm ngoài khối CEPT.

- Thuật toán A5/0 có thể được sử dụng khi trạm thu phát sóng chỉ định và đường truyền sẽ không được mã hóa. Điều đáng nói là người dùng ĐTDĐ không hề được biết là đường truyền của cuộc gọi hiện tại có được mã hóa hay không. Đây chính là nền tảng cho hình thức tấn công man-in-the-middle để nghe lén cuộc gọi.

Ngoài 3 thuật toán trên, thuật toán A5/3 là thuật toán mới nhất được phát triển để khắc phục các điểm yếu của A5/1 và A5/2.

1.2.2.2. Các nguy cơ mất an toàn

**** Nguy cơ tấn công ăn cắp, nhân bản SIM***

**** Nguy cơ tấn công nghe lén cuộc gọi bằng thủ thuật man-in-the-middle***

**** Nguy cơ tấn công nghe lén bằng thủ thuật giải mã thuật toán A5***

**** Nguy cơ tấn công giả mạo CALL-ID và giả mạo người gửi tin nhắn SMS***

**** Nguy cơ tấn công spam SMS, virus SMS***

**** Nguy cơ hacker sử dụng các phần mềm gián điệp trên ĐTDĐ***

1.3. Giải pháp kỹ thuật để bảo mật tin nhắn

Trong luận văn này, tôi tập trung nghiên cứu 3 hướng về giải pháp kỹ thuật bảo mật tin nhắn. Đầu tiên đó là giải pháp cung cấp dịch vụ bảo mật tin nhắn SMS peer-to-peer. Thứ hai, đó là các giải pháp cung cấp dịch vụ an ninh đó là: bảo mật, tính toàn vẹn, xác thực và

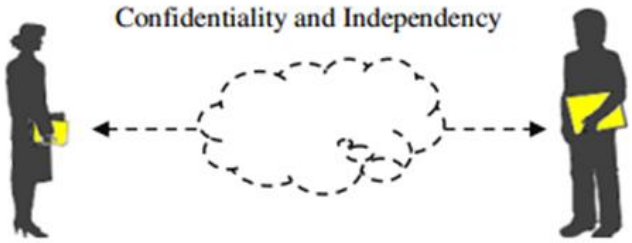
chống chối bỏ. Thứ ba, một số giải pháp phụ thuộc vào các nhà cung cấp dịch vụ hoặc các máy chủ điều hành mạng ĐTDĐ.

Năm 2003, Marko và Smile đã đề xuất phương pháp mã hóa dựa trên lý thuyết nhóm để bảo mật tin nhắn SMS. Họ sử dụng cùng một khóa cho mã hóa và giải mã. Vì thế chúng ta có thể xem chúng như một nhóm của một phương pháp mã hóa đối xứng. Giải pháp của họ cung cấp giải pháp bảo mật peer-to-peer nhưng nó không cung cấp xác thực người dùng và tính toàn vẹn của tin nhắn.

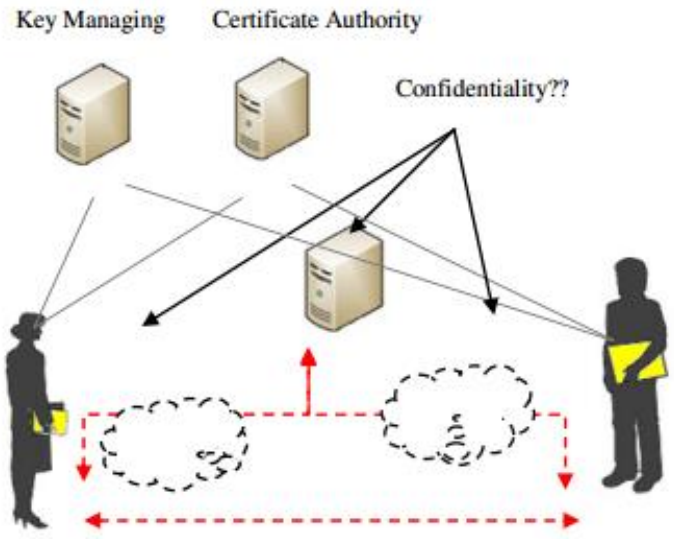
Năm 2004, Rathshinanga et al thì lại đề xuất một giao thức để giữ an toàn thông tin liên lạc tin nhắn SMS giữa khách hàng và máy chủ sử dụng các gói WMA. Họ đã sử dụng hệ mật mã bất đối xứng RSA và hệ mật mã đối xứng AES/CTR và chiến lược xác thực mật khẩu để đảm bảo tính bảo mật và tính toàn vẹn của thông tin liên lạc tin nhắn SMS. Giải pháp của họ được thiết kế để đảm bảo giao tiếp giữa người sử dụng và máy chủ. Nếu máy chủ bị một hacker tấn công, toàn bộ giao thức sẽ thất bại vì các hacker có thể ngụy trang như các bên hợp pháp bằng cách sử dụng các thông tin bị đánh cắp. Vì vậy, giải pháp này không phải là an toàn tuyệt đối. Hơn nữa, nó cung cấp sự bảo mật và tính toàn vẹn, nhưng các giải pháp không thể cung cấp một dịch vụ bảo vệ chống chối bỏ. Croft và Olivier, 2005 đã sử dụng pad một lần sử dụng thông tin chia sẻ giữa các đối tượng giao tiếp ngang hàng và các máy chủ GSM. Chìa khóa này được tạo ra từ các thông tin được chia sẻ này sử dụng kỹ thuật băm, đủ ngẫu nhiên để sử dụng trong thời gian xấp xỉ một pad. Các khóa này phải là duy nhất cho mỗi tin nhắn SMS, giả định rằng máy chủ GSM sẽ thay đổi tạm thời số nhận dạng thuê bao điện thoại (TMSI) cho mỗi tin nhắn SMS. Các SMS có thể được giải mã tại trung tâm chuyển mạch di động (MSC). Giải pháp này phụ thuộc vào các nhà điều hành mạng di động. Hơn nữa nó cũng không cung cấp mã hóa peer-to-peer vì tin nhắn có thể được giải mã trong mạng ĐTDĐ và được mã hóa một lần nữa, sau đó được gửi đến người nhận. Nếu một kẻ tấn công tăng quyền truy nhập vào mạng các nhà điều hành ĐTDĐ, tính bảo mật sẽ không còn vì các tin nhắn SMS là định dạng văn bản rất đơn giản.

Năm 2008, Lisonek và Dranhansky sử dụng mật mã bất đối xứng (RSA) để cung cấp tính bảo mật, tính toàn vẹn, tính xác thực và chống chối bỏ. Họ giả định rằng các cơ quan chứng nhận sẽ kiểm tra các chứng chỉ, và người sử dụng phải tải các chứng chỉ về từ máy chủ của cơ quan chứng nhận thông qua Internet. Nói chung giải pháp cung cấp an ninh SMS peer-to-peer cũng như đảm bảo tính bảo mật, tính toàn vẹn, xác thực và các dịch vụ an ninh chống chối bỏ. Tuy nhiên, sự phụ thuộc vào một cơ quan chứng nhận sẽ làm phức tạp giải pháp được

thực hiện cho các cá nhân. Anuer et al. (2008) đề xuất các giải pháp mã hóa tin nhắn SMS/MMS. Họ sử dụng cả hai thuật toán mật mã đối xứng (AES) và thuật toán mã hóa không đối xứng (RSA). Đối với hệ mật mã bất đối xứng, người dùng phải chấp nhận một chứng chỉ số với máy chủ của cơ quan chứng nhận trước khi bắt đầu sử dụng giải pháp này. Sau khi máy chủ cung cấp chứng chỉ, người dùng phải duyệt khóa công khai mã hóa thư mục trên máy chủ để tải khóa công khai về. Thư mục này sẽ cung cấp thông tin về tất cả chứng chỉ của người dùng và tình trạng của nó. Tuy nhiên, giải pháp của họ cung cấp tính bảo mật, tính toàn vẹn, xác thực và chống chối bỏ nhưng nó phụ thuộc vào máy chủ xác nhận chứng chỉ để tạo ra các mật mã và xác nhận người dùng.



Hình 1.11. Mã hóa đối xứng với cơ sở vật chất không máy chủ



Hình 1.12. Mã hóa bất đối xứng với cơ sở vật chất có máy chủ

Toorani và Shirazi (2008) đã giới thiệu một giao thức an toàn trên lớp ứng dụng được gọi là SSMS. Giao thức này có thể được sử dụng để nhúng các thuộc tính bảo mật mong muốn vào trong các tin nhắn SMS. Nó cung cấp giải pháp khóa công khai dựa trên đường cong Elliptic (ECC) để sử dụng khóa công khai cho việc tạo khóa bí mật của hệ mật mã đối xứng. Tuy nhiên nó dựa vào máy chủ của bên thứ ba có nghĩa là KGS, (Key Generating Server), máy chủ OCSP (Online Certificate Status Protocol) như một phần của giải pháp.

Zhao et al. (2008) đề xuất một giải pháp mới cho kênh bảo mật tin nhắn sử dụng mật mã dựa trên nhận dạng. Giải pháp này cung cấp tính bảo mật peer-to-peer từ nhà cung cấp dịch vụ cho người sử dụng ĐTDĐ, và giữa những người sử dụng ĐTDĐ với nhau. Mật mã dựa trên nhận dạng quy định một hệ mật mã trong đó cả khóa công khai và khóa bí mật đều dựa trên nhận dạng của người dùng. Giải pháp này có khóa công khai của người dùng là một chức năng được tính toán dễ dàng bởi các đặc điểm nhận dạng của người dùng, trong khi khóa riêng của người dùng được tính toán bởi một cơ quan đáng tin cậy, được gọi là bộ sinh khóa riêng (PKG). Mật mã dựa trên nhận dạng cần một giai đoạn thiết lập trong đó các thông số của hệ thống được phân phối tới người sử dụng nó. Các thông số này bao gồm khóa công khai của hệ thống, khóa chủ, khóa riêng của mỗi người dùng, và các thuật toán được sử dụng để mã hóa và giải mã cũng như hàm băm. Giải pháp này mang lại tính toàn vẹn, bảo mật và xác thực của tin nhắn SMS bằng cách gắn một tin nhắn với một người cụ thể. Tuy nhiên nó không mang lại tính chống chối bỏ khi các nhà cung cấp dịch vụ cung cấp các khóa riêng để một người sử dụng, do đó người sử dụng chỉ đơn giản là có thể phủ nhận đã gửi tin nhắn đã ký với khóa riêng của mình. Hơn nữa, giải pháp này phụ thuộc vào các nhà điều hành mạng di động, điều này gây khó khăn đối với người sử dụng.

Wu và Tan (2009b) đề xuất một giao thức truyền thông bảo mật cho tin nhắn SMS. Họ đã sử dụng thuật toán không đối xứng RSA-1024 và AES và thuật toán đối xứng 3DES để cung cấp một kênh an toàn peer-to-peer giữa máy chủ và thiết bị đầu cuối di động. Họ sử dụng thuật toán MD5 và SHA1 để kiểm tra tính toàn vẹn của tin nhắn. Do sử dụng mật mã đối xứng và thuật toán hàm băm, họ có thể đảm bảo tính bảo mật, tính toàn vẹn và chống chối bỏ tin nhắn SMS. Tuy nhiên, giải pháp này là giải pháp dựa trên máy chủ, chỉ có thể được thực hiện bởi các nhà điều hành mạng di động. Theo một số tài liệu mà tôi đã nghiên cứu thì một số người sử dụng mật mã đối xứng như một giải pháp có thể cung cấp tính bảo mật cho tin nhắn SMS. Có nhiều điều tranh cãi khi mật mã đối xứng không thể cung cấp xác thực người gửi, chống chối bỏ và tính toàn vẹn của tin nhắn. Một số nhà nghiên cứu khác đã đề xuất sử dụng mật mã bất đối xứng để cung cấp tính bảo mật, xác thực, tính toàn vẹn và chống chối bỏ của dịch vụ tin nhắn SMS. Tuy nhiên, đây cũng không phải là giải pháp tốt nhất vì mật mã bất đối xứng đòi hỏi rất nhiều sự tính toán và lưu trữ nguồn để tính toán cũng như việc lưu trữ các khóa công cộng và tư nhân.

CHƯƠNG 2: ỨNG DỤNG MÃ HÓA TRONG BẢO MẬT TIN NHẮN NGẮN SMS

Chương này của luận văn sẽ đi sâu vào tìm hiểu một số thuật toán mã hóa được sử dụng cho việc bảo mật tin nhắn đang được áp dụng hiện nay.

2.1. Ứng dụng thuật toán AES trong bảo mật tin nhắn

2.1.1. Thuật toán AES

2.1.1.1. Nguồn gốc của thuật toán AES

2.1.1.2. Yêu cầu của AES

2.1.1.3. Tiêu chuẩn triển khai của AES

2.1.1.4. Chuẩn mã nâng cao AES – Rijndael

Cuối cùng Rijndael được chọn là chuẩn mã nâng cao. Nó được thiết kế bởi Rijmen – Daemen ở Bỉ, có các đặc trưng sau:

- Có 128/192/256 bit khoá và 128 bit khối dữ liệu.
- Lặp hơi khác với Fiestel
- Chia dữ liệu thành 4 nhóm – 4 byte
- Thao tác trên cả khối mỗi vòng
- Thiết kế để:

+ Chống lại các tấn công đã biết

+ Tốc độ nhanh và nén mã trên nhiều CPU

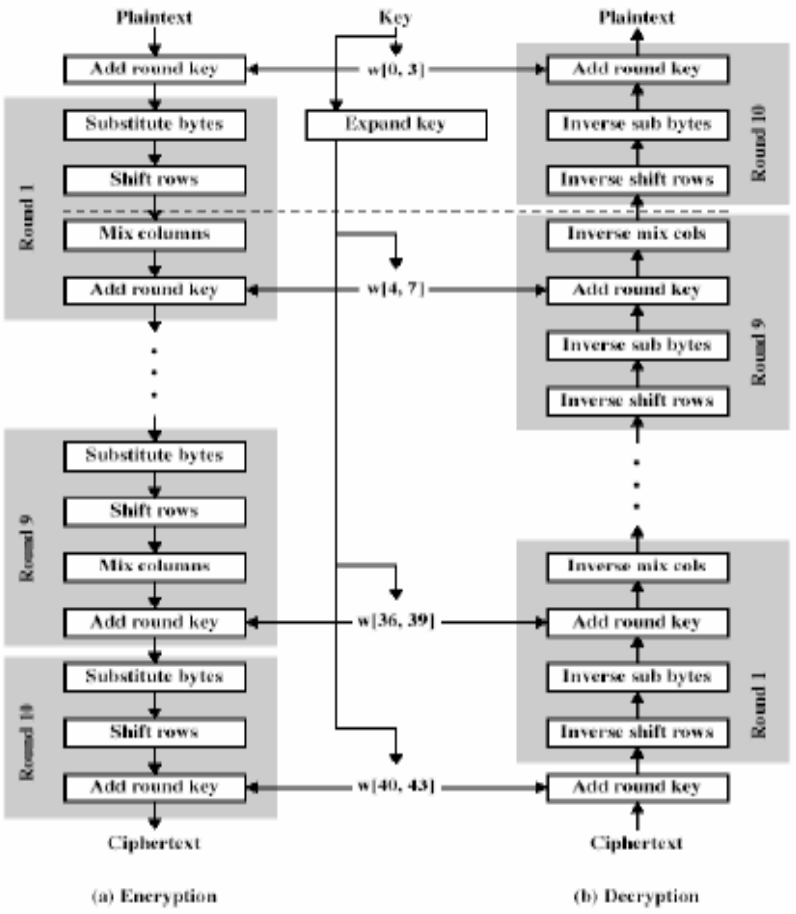
+ Đơn giản trong thiết kế

+ Xử lý khối dữ liệu 128 bit như 4 nhóm của 4 byte: 128 = 4*4*8 bit. Mỗi nhóm nằm trên một hàng. Ma trận 4 hàng, 4 cột với mỗi phần tử là 1 byte coi như trạng thái được xử lý qua các vòng mã hoá và giải mã.

+ Khoá mở rộng thành mảng gồm 44 từ 32 bit w[i].

+ Có tùy chọn 9/11/13 vòng, trong đó mỗi vòng bao gồm

- Phép thế byte (dùng một S box cho 1 byte)
- Dịch hàng (hoán vị byte giữa nhóm/cột)
- Trộn cột (sử dụng nhân ma trận của các cột)
- Cộng khoá vòng (XOR trạng thái dữ liệu với khoá vòng).
- Mọi phép toán được thực hiện với XOR và bảng tra, nên rất nhanh và hiệu quả.



Hình 2.1. Sơ đồ Rijndael

2.1.2. Ứng dụng thuật toán AES trong bảo mật tin nhắn SMS

Trong khuôn khổ luận văn này, tôi nghiên cứu ứng dụng của thuật toán AES trong bảo mật tin nhắn SMS trên nền Android. Ứng dụng được tạo ra đảm bảo có thể cài đặt được vào điện thoại di động và đảm bảo không có sự chậm trễ trong sử dụng các chương trình khác. Giao diện người dùng được tạo ra phải đảm bảo đơn giản và thân thiện với người dùng. Ứng dụng này được sử dụng để xác thực người gửi tin nhắn, phát hiện nếu tin nhắn bị hỏng hoặc bị giả mạo trong quá trình truyền. Quan trọng nhất, tin nhắn có chứa thông tin nhạy cảm được lưu trữ an toàn và không bị tiết lộ ngay cả khi thiết bị bị kẻ tấn công truy nhập vào. Điểm độc đáo và quan trọng nhất là sự an toàn của dữ liệu được mã hóa chống lại các cuộc tấn công khác nhau. Ứng dụng đảm bảo sự an toàn của dữ liệu trong quá trình truyền mà không có bất cứ phân đoạn dữ liệu nào bị hỏng.

2.1.2.1. Ứng dụng của thuật toán AES hoạt động theo cách sau đây:

i) Người dùng mở ứng dụng và xác thực sử dụng khóa mẫu.

ii) Người dùng có thể nhập tin nhắn mới hoặc trả lời một tin nhắn đến.

iii) Nếu chọn soạn thảo một tin nhắn mới, người dùng nhập vào tin nhắn và nhấn nút mã hóa sau khi nhập tên của người nhận. Người dùng phải nhập một khóa của mật mã trước khi tin nhắn được gửi đi. Chìa khóa mật mã được tự động tạo ra khi người dùng không nhập khóa.

iv) Nếu người dùng chọn trả lời một tin nhắn hiện tại, người đó phải giải mã được tin nhắn, sau đó nhập tin nhắn trả lời. Hệ thống sẽ yêu cầu người dùng nhập chìa khóa của mật mã trước khi tin nhắn được gửi.

v) Khi chìa khóa của mật mã được nhập vào, tin nhắn được gửi đi thành công và được thể hiện ở dạng mã hóa trong phần chủ đề.

2.1.2.2. Mục tiêu của ứng dụng

Các mục tiêu chính của ứng dụng này là:

- Phát triển một ứng dụng tin nhắn SMS an toàn
- Duy trì thông tin được mã hóa của tin nhắn người nhận
- Bảo vệ chống lại lạm dụng thông tin tin nhắn
- Bảo mật cao và cải thiện an ninh.

2.1.2.3. Giả mã của ứng dụng trên nền Android

2.2. Ứng dụng mật mã dựa trên định danh trong bảo mật tin nhắn

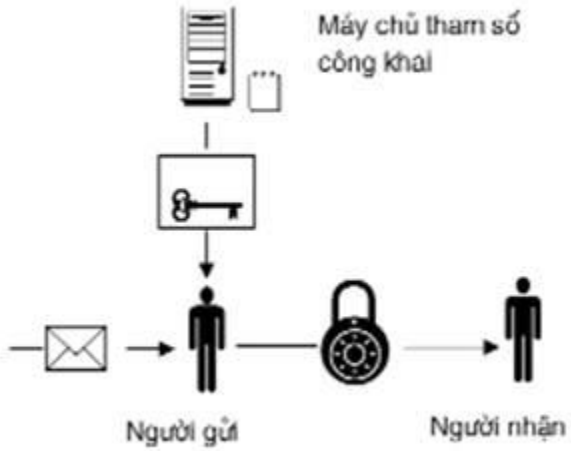
2.2.1. Mật mã dựa trên định danh

2.2.1.1. Khái quát về Mã hoá dựa trên định danh (Indetity-based encryption - IBE)

2.2.1.2. Hệ thống khóa công khai truyền thống

2.2.1.3. Lược đồ mã hóa dựa trên định danh

IBE lần đầu tiên được Adi Shamir nói tới vào năm 1984, khi ông mô tả một cách khái lược về các tính chất và cách thức sử dụng một hệ thống như vậy. Mặc dù ông chưa thực hiện được một công nghệ an toàn và khả thi hoạt động như đã mô tả, song các ưu thế về khả năng sử dụng của IBE so với các công nghệ khác đã được ông mô tả như sau:



Hình 2.8. Mã hoá bằng hệ thống IBE

Một hệ thống IBE có các điểm tương tự với các hệ thống khoá công khai truyền thống, nhưng cũng có nhiều điểm khác biệt. Trong khi các khoá công khai truyền thống chứa tất cả các tham số cần thiết để sử dụng khoá, thì để sử dụng một hệ thống IBE, người sử dụng thông thường cần nhận được một tập các tham số công khai từ một bên thứ ba tin cậy. Cùng với những tham số này, người sử dụng có thể tính khoá công khai IBE của người sử dụng bất kỳ khác và dùng nó để mã hoá thông tin gửi tới người đó (Hình 2.8).

Người nhận thông tin đã được mã hoá bởi IBE sau đó xác thực theo một cách nào đó với bộ tạo khoá bí mật (PKG- private key generator). Một bên thứ ba tin cậy tính được khoá bí mật IBE tương ứng với một khoá công khai IBE cụ thể. Bộ tạo khoá bí mật thường sử dụng thông tin bí mật, được gọi là bí mật chủ (master secret) cộng với định danh của người sử dụng để tính ra khoá bí mật. Sau khi khoá bí mật đó được tính ra, nó được phân phối một cách an toàn tới người sử dụng có thẩm quyền (Hình 2.9).

Hình 2.9. Giải mã bằng hệ thống IBE

2.2.1.4. Các thuật toán sử dụng trong IBE

Bảng 2.2. Bốn thuật toán tạo nên lược đồ IBE

Thuật toán	Tóm tắt
Thiết lập	Khởi tạo tất cả các tham số hệ thống
Trích	Tính khoá bí mật IBE từ bí mật chủ của bộ tạo khoá bí mật và định danh nhờ sử dụng các tham số hệ thống
Mã hoá	Mã hoá thông tin nhờ sử dụng khoá công khai IBE đã tính được từ các tham số hệ thống và định danh
Giải mã	Giải mã thông tin nhờ sử dụng khoá bí mật IBE đã tính được từ bí mật chủ của bộ tạo khoá bí mật PKG và định danh

2.2.1.5. Các mục tiêu an toàn

Có 5 mục tiêu chính mà một giải pháp an toàn thông tin có thể đáp ứng: cung cấp tính bí mật, tính toàn vẹn, tính sẵn sàng, tính xác thực và tính không chối bỏ. IBE cung cấp một giải pháp dễ thực thi mà vẫn đảm bảo tính bí mật của dữ liệu. Nó không bảo đảm tính toàn vẹn, tính sẵn sàng, tính xác thực và không chối bỏ. Chúng được cung cấp dễ hơn bởi các chữ ký số nhờ các khoá đã được tạo ra và quản lý bởi hệ thống khoá công khai truyền thống. Các ưu thế mà IBE cung cấp làm cho nó là một giải pháp rất tốt cho một số trường hợp ứng dụng. Một giải pháp pha trộn sử dụng IBE cho mã hoá và hệ thống khoá công khai truyền thống để cung cấp các chữ ký số có thể là một giải pháp kết hợp được những đặc tính tốt nhất của mỗi công nghệ.

2.2.2. Ứng dụng mã hóa dựa trên định danh vào bảo mật tin nhắn

2.2.2.1. Lý do chọn mã hóa dựa trên định danh

Các yêu cầu tài nguyên tính toán được so sánh với PKC cho các khóa cùng kích cỡ. Tuy nhiên nó yêu cầu các khóa ngắn hơn để đạt được cùng một mức bảo mật khi so sánh với kích cỡ khóa của hệ thống mật mã sử dụng khóa công khai. Hơn nữa, nó không yêu cầu sự luân chuyển và lưu trữ của các khóa công khai. SP cần duy trì n khóa nếu có n người dùng. Mỗi người dùng không cần duy trì khóa cho SP, và cũng không cần duy trì bất cứ thứ gì khác trong giao tiếp user-to-user. Một nhược điểm của mã hóa dựa trên định danh là nó vẫn còn trong giai đoạn nghiên cứu, không có nhiều khách hàng thương mại. Từ phân tích trên, ta thấy rằng các ứng dụng cho điện thoại di động khi sử dụng mật mã khóa đối xứng và mật mã khóa công khai là không phù hợp do yêu cầu của bộ nhớ lớn, đặc biệt là trong giao tiếp user-to-user.

2.2.2.2. Nhận dạng

Ưu điểm của mã hóa dựa trên định danh là không cần phổ biến khóa công khai trước khi giao tiếp, và vì thế không cần phải lưu trữ khóa. Khóa công khai nên để ẩn với tin nhắn. Trong GSM/UMTS, danh tính người dùng chính là thuê bao di động quốc tế (IMSI). Lưu ý là số IMSI không phải là số thuê bao (MSISDN). Các số MSISDN là một số điện thoại đầy đủ đầu số quốc tế và được kết hợp với số IMSI trong cơ sở dữ liệu đang sử dụng. Số MSISDN là các thông tin công khai trong khi số IMSI được dành cho định danh nội bộ của hệ thống và định tuyến kết quả. Chúng tôi chọn MSISDN như là danh tính được sử dụng trong mã hóa dựa trên định danh cho người sử dụng điện thoại di động, bởi vì số của người nhận được người gửi biết khi gửi tin nhắn cho người nhận, và số của người gửi được người nhận biết khi nhận được tin nhắn đến.

Trong mạng di động, mỗi nhà cung cấp dịch vụ có một số ngắn độc nhất mà được công khai cho người dùng điện thoại. Số này được sử dụng cho người dùng truy nhập khi gửi tin nhắn SMS hoặc MMS. Chúng tôi chọn số này như là danh tính được sử dụng trong mã hóa dựa trên định danh.

2.2.2.3. Cài đặt hệ thống

Mã hóa dựa trên định danh cần có một giai đoạn thiết lập, trong đó thông số hệ thống được phân phối cho người sử dụng của nó. Những thông số này bao gồm khóa công khai, khóa chủ, khóa bí mật của mỗi người dùng và thuật toán được sử dụng cho hàm băm, mã hóa và giải mã.

Tôi sử dụng phương pháp mã hóa này để cung cấp tính toàn vẹn, tính bảo mật, tính xác thực và chống chối bỏ cho dịch vụ tin nhắn ngắn SMS. Hệ mật này dựa trên sự làm việc được đơn giản hóa để dành cho những yêu cầu của điện thoại di động. Các chức năng của nhà cung cấp dịch vụ như là người quản trị khóa. Tại giai đoạn cài đặt hệ thống, SP tạo khóa công khai của hệ thống P_{pub} như sP nơi s là một số ngẫu nhiên trong Z^*_q và P là một điểm tùy ý trong E/F_p của trật tự q. Nó cũng chọn một hàm băm mật mã $G:\{0,1\}^* \to F$ để ánh xạ các chuỗi danh tính có thể biến đổi được tới các điểm trong E/F_p và chọn hàm băm $H_1 : F_{p^2} \to \{0,1\}^n$ và $H_2 : F_{p^2} \to Z_q$ cho khóa có chiều dài theo quy định.

$H_3 : \{0,1\}^n \times \{0,1\}^n \to F_q, \quad H_4 : F_q \times G_2 \to \{0,1\}^n, \quad và\ H_5 : \{0,1\}^n \to \{0,1\}^m$

Khóa chủ ban đầu $s \in Z_q$ và các thông số của hệ thống $params = \langle p, n, P, P_{pub}, G, H_1, H_2 \rangle$ $(H_3, H_4 và\ H_5)$ được xác định rõ và được tính toán bởi nhà

cung cấp dịch vụ. Để đưa ra chuỗi $ID \in \{0,1\}^*$ của một .nút, phương pháp mã hóa xây dựng một khóa bí mật ban đầu d_{ID} như $d_{ID} = sQ_{ID}$ trong đó Q_{ID} là một điểm trong E/F_p được ánh xạ trong tập ánh xạ E/F_p được ánh xạ từ ID. Mỗi người dùng nhận những thông số cua hệ thống và khóa bí mật của nó từ nhà cung cấp dịch vụ khi họ đăng ký dịch vụ. Mỗi dịch vụ với số ngắn độc nhất được coi như là một người dùng duy nhất và nhận được khóa bí mật độc nhất của nó. Để ngăn chặn một điện thoại bị mất đang được sử dụng một cách gian lận, người dùng điện thoại phải chứng minh sở hữu hợp pháp của số điện thoại họ đang sử dụng. Để đảm bảo tính bí mật end-to-end, khóa bí mật cần được phân phối trong một kênh khác SMS.

Một add-on Message Manager Tookit, bao gồm các ứng dụng mã hóa và giải mã, các thông số của hệ thống và khóa bí mật được thiết lập trong điện thoại di động khi người dùng đăng ký dịch vụ. Ngày nay, điện thoại di động hầu hết đều hỗ trợ người dùng các ứng dụng . Java 2 Micro Edition (J2ME) là một nền tảng Java cung cấp một môi trường tiêu chuẩn cho phát triển các ứng dụng phù hợp để chạy trên các thiết bị di động. J2ME cung cấp một gói tùy chọn được gọi là Wireless Messaging API (WMA) cho phép các ứng dụng điện thoại di động gửi và nhận các tin nhắn không dây. Nó cung cấp tin nhắn nhị phân, tuy nhiên nó không cung cấp bất kỳ ứng dụng mã hóa/giải mã tin nhắn. Chúng tôi đề nghị sử dụng J2ME WMA cùng với sự tăng cường an ninh cho các chương trình trên ĐTDĐ.

Về phía nhà cung cấp dịch vụ, một ứng dụng tương ứng chạy trên máy chủ của nó. Các ứng dụng mã hóa tất cả các tin nhắn trước khi gửi đến SMSC và giải mã các tin nhắn đến từ SMSC.

2.2.2.4. Một đề án cơ bản để bảo mật tin nhắn SMS

Sau Message Management Toolkit cùng với các thông số của hệ thống được thiết lập trong một thiết bị di động, nó có thể giao tiếp an toàn với các SP, hoặc các thiết bị di động khác từ cùng một SP. Message Management Toolkit mã hóa một tin nhắn với các thông số của hệ thống nếu cần thiết.

Một tin nhắn SMS được xác định là duy nhất bởi các định danh của người gửi – mã số MSISDN hoặc số ngắn trong tiêu đề của thông báo. Một thiết bị đích cũng có thể được định danh bởi ID của nó (MSISDN hoặc số ngắn). Vì thế một chìa khóa của mật mã được sử dụng trong mã hóa dựa trên định danh có thể được xác định bằng cách sử dụng hai danh tính. Khi người dùng A gửi tin nhắn SMS cho người dùng B (hoặc B có thể là SP), nó mã hóa và xác thực tin nhắn như sau:

1) Đầu tiên, tạo ra một khóa chia sẻ ẩn với B, không có bất kỳ sự tương tác với B: $k = H_1(g^r)$ trong đó:

$g = \hat{e}(d_A, Q_B), \quad r = H_2[Q_A, Q_B], \quad Q_A = G(ID_A), \quad Q_B = G(ID_B), \quad d_A = sQ_A.ID_B$ là MSISDN hoặc số ngắn của người nhận mà người nhận dự định để gửi tin nhắn.

2) Tải trọng mã hóa của tin nhắn M: $C = M \oplus k$. Tin nhắn đã được mã hóa C được đặt trong trường tải trọng. Gói mã hóa được giao cho nhà điều hành mạng. Sau khi nó truyền qua mạng Internet và mạng di động, tại phía người nhận B, tin nhắn được giải mã như sau:

Bước 1: Đầu tiên, B tạo ra một khóa chia sẻ ẩn với A, không có bất kỳ sự tương tác nào với A: $k = H_1(g^r)$ trong đó:

$g = \hat{e}(Q_A, d_B), \quad r = H_2[\hat{e}(Q_A, Q_B)], \quad Q_A = G(ID_A), \quad Q_B = G(ID_B), \quad d_B = sQ_B$. Chú ý rằng ID_A là MSISDN của người gửi có nguồn gốc từ tiêu đề của gói tin và $\hat{e}(Q_A, d_B) = \hat{e}(d_A, Q_B)$

Bước 2: B giải mã tải trọng của tin nhắn C: $M' = C \oplus k$. Tin nhắn được giải mã M' tương đương với tin nhắn gốc M.

Quá trình mã hóa và giải mã cũng cung cấp tính xác thực, vì tin nhắn được mã hóa tại phía người gửi với khóa bí mật của họ và khóa công khai của người nhận.. Phần mào đầu của tin nhắn được bảo vệ bởi cơ chế bảo mật truy cập của mạng di động. Công nghệ bảo mật truy cập (thực hiện hoặc thiết kế) đảm bảo các thông tin truyền từ MSC tới trạm gốc, và từ trạm gốc tới các thiết bị di động được mã hóa và không thể bị giả mạo. Cũng trong 3G, các thiết bị di động và trạm gốc được xác thực bằng hai cách, vì thế không trạm gốc giả mạo nào có thể đóng vai như một trạm gốc xác thực được. Trên cơ sở công nghệ bảo mật truy cập, ứng dụng này đưa ra thêm một cách để bảo mật end-to-end từ SP đến một thiết bị đầu cuối.

2.2.2.5. Một đề án cải tiến để bảo mật tin nhắn SMS

Đề án cơ bản trên dựa nhiều vào bảo mật truy cập của các mạng di động và không thể xác minh tính toàn vẹn của tin nhắn.

Để cải thiện mức độ bảo mật của nó, chúng ta cần không gian trong gói tin để chứa chữ ký số và các thông số của thuật toán. Khi chữ ký số được đánh dấu với khóa bí mật của người gửi được sử dụng một cách rộng rãi trên Internet để bảo vệ tính toàn vẹn và xác thực của dữ liệu, như là email và URLs và nó cũng không dễ để sử dụng trong tin nhắn SMS. Lý do là các gói tin của SMS thường rất ngắn (140 bytes) và cơ chế giống như các gói tin IP. Giao diện SMS trong hầu hết các điện thoại phân mảnh và tương tự tại lớp ứng dụng tin nhắn nếu quá dài để gửi trong một gói tin SMS. Ví dụ WMA tự cung cấp sự phân mảnh và sự tập

hợp lại các tin nhắn. Tất cả các mảnh được phân phối tới địa chỉ cá nhận xác định. Tại phía người trả lời, nó tự động tập hợp lại các phân mảnh thành một tin nhắn đầy đủ trước khi trả nó về cho ứng dụng.

Một giải pháp xa hơn thì nhu cầu về không gian dành cho chữ ký số và các thông số bảo mật càng lớn. Các thông số bảo mật có thể chứa các giá trị có ích như là Sequence Number hoặc Timestamp. Đầu tiên, các thông số bảo mật được nối vào tin nhắn khi toàn bộ tin nhắn được xử lý. Sau đó, tin nhắn được mã hóa, chữ ký số được tính toán và được nối vào tin nhắn sau cùng.

Khi người dùng A gửi một tin nhắn tới người dùng B (A hoặc B có thể là SP), nó mã hóa và xác thực tin nhắn như sau:

Bước 1: Đầu tiên tạo một khóa chia sẻ ẩn với B, không tương tác với B: $k = H_1\left(g^r\right)$ trong đó:

$$g = \hat{e}(d_A, Q_B), \quad r = H_2[Q_A, Q_B], \quad Q_A = G(ID_A), \quad Q_B = G(ID_B), \quad d_A = sQ_A.ID_B$$

là MSISDN hoặc số ngắn của người nhận mà người gửi định gửi tin nhắn đến.

Bước 2: A mã hóa tin nhắn M (giảm tải trọng), và văn bản được mã hóa đầu ra $C = E_{H_5(k)}(M)$ trong đó E_k là một chức năng hệ mật mã đối xứng an toàn.

Bước 3: A đánh dấu tin nhắn với khóa bí mật của mình và khóa công khai của người nhận: $\sigma = H_3(C,k), S = H_4(\sigma, g)$. Tin nhắn được mã hóa C và chữ ký số S được đặt trong trường tải trọng của gói tin SMS tiêu chuẩn, $M' = \langle C, S \rangle$.

Tại phía người nhận B, tin nhắn được xác minh và giải mã như sau:

Bước 1: Đầu tiên, B tạo ra khóa chia sẻ ẩn với A, không tương tác với A: $k = H_1(g^r)$ trong đó

$$g = \hat{e}(Q_A, d_B), \quad r = H_2[\hat{e}(Q_A, Q_B)], \quad Q_A = G(ID_A), \quad Q_B = G(ID_B), \quad d_B = sQ_B.$$

Chú ý rằng ID_A là MSISDN của người gửi có nguồn gốc từ tiêu đề của gói tin và $\hat{e}(Q_A, d_B) = \hat{e}(d_A, Q_B)$.

Bước 2: Để tin nhắn đã nhận $M' = \langle C, S \rangle$ trong định dạng đã được định nghĩa với chữ ký số S và văn bản mã hóa C, chữ ký số được xác minh: $\sigma' = H_3(C,k), S' = H_4(\sigma', g)$. Nếu S phù hợp với kết quả tính toán mới S', tính toàn vẹn và tính xác thực được xác nhận, và tin nhắn được xử lý tốt hơn. Nếu không, tin nhắn bị loại bỏ.

Bước 3: Để nhận tin nhắn, B giải mã nó với khóa được chia sẻ: $M''= D_{H_5(k)}(C)$, trong đó D_k là một chức năng hệ mật mã bất đối xứng an toàn. M'' nên tương tự như tin nhắn gốc M.

Đề án này với độ an toàn được cái tiến tăng độ dài của một tin nhắn do việc bổ sung chữ ký số và các thông số bảo mật (M' so sánh với M). Và số lượng gói tin tương ứng với tin nhắn gốc có thể tăng thêm 1. Sự trễ cũng có thể xảy ra vì tất cả những phân mảnh phải chờ cho chữ ký số và các thông só bảo mật đến trước khi tập hợp và khôi phục lại tin nhắn gốc. Vì thế tốt hơn là thuật toán mã hóa vừa nén được các tin nhắn mã hóa và không tăng chiều dài cuối cùng.

2.3.2.6. Sử dụng hệ thống

Message Management Toolkit không thay đổi giao diện nhắn tin truyền thống trên điện thoại di động, nhưng nó được xây dựng trên trang đầu của chúng. Nó giống như một giao diện quản lý tin nhắn mới, người dùng có thể nhận và gửi tất cả các tin nhắn. Người dùng chọn một tùy chọn để đọc hoặc gửi tin nhắn như tin nhắn mã hóa hoặc tin nhắn văn bản đơn giản. Một tin nhắn mã hóa có nhúng một cờ đặc biệt, để thông báo cho các ứng dụng nếu không các ứng dụng sẽ tự động xử lý nó. Khóa bí mật tương ứng với MSISDN của điện thoại di động chứ không phải tương ứng với người dùng. Để ràng buộc các khóa bí mật với người dùng, ứng dụng sẽ được bảo vệ bởi một password được người dùng đặt khi sử dụng lần đầu. J2ME Mobile Information Device Profile (MIDP) cung cấp một tính năng lưu trữ liên tục (Persistent Storage) để đảm bảo rằng bản ghi được ứng dụng Java tạo nên chỉ được một mình nó truy nhập. Độ an toàn của password được tính năng này bảo vệ.

Trong tất cả các giao tiếp, chỉ các nhà điều hành mạng có quyền truy nhập văn bản mã hóa. Bất kỳ ai chặn đường truyền hoặc khai thác mạng thì đều chỉ nhìn thấy tin nhắn được mã hóa và không thể có được văn bản rõ ràng như văn bản gốc được.

2.3. Ứng dụng mật mã trên đường cong Elliptic trong bảo mật tin nhắn

2.3.1. Mật mã trên đường cong Elliptic

2.3.2. Ứng dụng hệ mật trên đường cong Elliptic trong bảo mật tin nhắn

i) Hoạt động của hệ thống bảo mật tin nhắn sử dụng mật mã trên đường cong Elliptic

Hệ thống sẽ sử dụng các khái niệm về mật mã trên đường cong Elliptic để mã hóa các tin nhắn và gửi trên một kênh chung. Người gửi viết một tin nhắn và nhập vào số điện thoại của người nhận. Khi người gửi gửi tin nhắn, thật toán được kích hoạt trên cả hai thiết bị di

động. Các khóa được tạo ra và chia sẻ giữa các thiết bị và mã hóa diễn ra cho tới khi kết thúc việc gửi. Sau khi mã hóa, tin nhắn được gửi tới người nhận và người đó giải mã nó bằng cách sử dụng khóa của mình để đọc tin nhắn.

Các phương pháp mã hóa và giải mã trong ECC được thiết kế để mã hóa và giải mã một điểm trên đường cong và không phải là toàn bộ tin nhắn. Trong quá trình mã hóa, mỗi ký tự trong tin nhắn được chuyển đổi thành các byte sau đó các byte thành các điểm có dạng (x, y) và sau đó các điểm phải được mã hóa bằng cách ánh xạ từng điểm đó với mỗi điểm trên đường cong Elliptic. Sau đó toàn bộ các điểm mã hóa này được khôi phục lại thành các byte và thành các chuỗi ký tự của SMS.

Khi tin nhắn được truyền đến người nhận, trong suốt quá trình giải mã, các chuỗi ký tự được khôi phục thành các byte; các byte này được giải mã thành các điểm sử dụng kỹ thuật ánh xạ và sau đó các điểm thành các byte và cuối cùng thành những ký tự của tin nhắn và chỉ sau khi văn bản được giải mã thì người nhận mới có thể xem được tin nhắn.

CHƯƠNG 3: XÂY DỰNG CHƯƠNG TRÌNH BẢO MẬT TIN NHẮN TRÊN ĐIỆN THOẠI DI ĐỘNG

Trong chương này, luận văn sẽ trình bày về cách thức để xây dựng chương trình bảo mật tin nhắn trên ĐTDĐ bằng ngôn ngữ Java với cộng nghệ J2ME kết hợp với sử dụng thư viện mã hóa Bouncy Castle để tạo chương trình mã hóa.

3.1. Xây dựng chương trình bảo mật tin nhắn trên điện thoại di động

3.1.1. Môi trường để lập trình

3.1.1.1. Java Development Kit (JDK)

3.1.1.2. Wireless Toolkit (WTK)

3.1.1.3. Bouncy Castle

3.1.1.4. ProGuard

3.1.2. Sử dụng thư viện Bouncy Castle để mã hóa trong ứng dụng di động

3.1.2.1. Khái quát về Bouncy Castle

3.1.2.2. Cài đặt Bouncy Castle

3.1.3. Mã hóa chuỗi văn bản trong chương trình SecureSMS

Dưới đây sẽ mô tả các bước mã mã hóa chuỗi văn bản trong chương trình bảo mật tin nhắn điện thoại di động SecureSMS:

3.1.3.1. Các bước mã hóa một chuỗi văn bản:

Bước 1: Chọn công cụ mã hóa và cấp một thể hiện cho công cụ mã hóa

Bước 2: Lưu trữ các văn bản được mã hóa trong một mảng byte

Bước 3: Khởi tạo các thuật toán với một khóa

Bước 4: Gọi công cụ mã hóa để mã hóa dữ liệu

3.1.3.2. Giải mã dữ liệu:

Các bước để giải mã dữ liệu:

Bước 1: Lưu trữ các văn bản cần được giải mã trong một mảng byte

Bước 2: Khởi tạo các thuật toán với một khóa

Bước 3: Gọi cho công cụ để giải mã dữ liệu

3.1.4. Tạo ứng dụng mã hóa tin nhắn điện thoại - SecureSMS

Dưới đây là các bước mà luận văn sẽ làm theo để tạo ra các MIDlet trong WTK:

***Bước 1*:** Tạo dự án mới

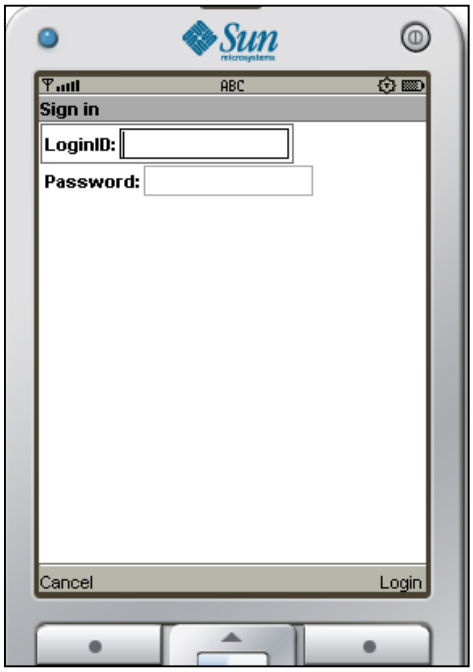
***Bước 2*:** Thêm vào ứng dụng thư viện Bouncy Castle

Bước 3: Viết mã nguồn cho chương trình:

Bước 4: Biên dịch chương trình

Bước 5: Thực thi chương trình SecureSMS:

Kết quả của chương trình SecureSMS được cho bởi hình sau:



Hình 3.11: Thực thi trình SecureSMS bằng công cụ WirelessToolkit

3.1.5. Obfuscation

3.1.5.1. Khái quát về obfuscation

3.1.5.2. Giải thích obfuscation

3.1.5.3. Cài đặt ProGuard

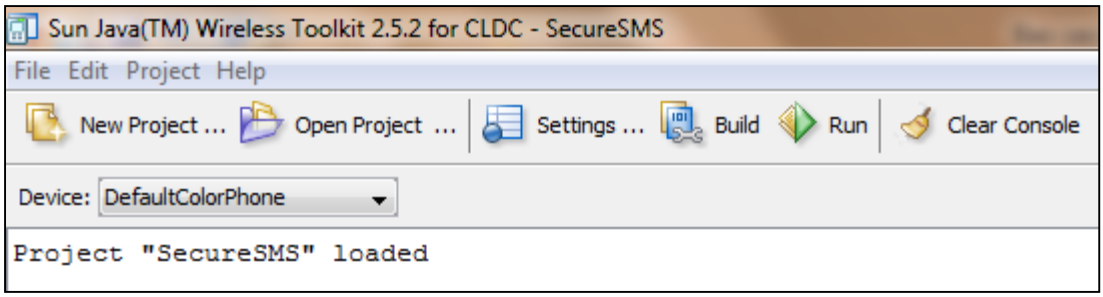
3.1.5.4. Đầu ra của Obfuscator

3.2. Thử nghiệm demo chương trình bảo mật tin nhắn trên ĐTDĐ

3.2.1. Thử nghiệm chương trình trên máy tính bằng WTK

3.2.1.1. Mở dự án SecureSMS

Khởi động chương trình Wireless Toolkit và tại cửa sổ của chương trình, chọn Open Project và sau đó chọn dự án SecureSMS để mở chương trình mã hóa tin nhắn điện thoại di động



Hình 3.16: Mở dự án SecureSMS

3.2.1.2. Thi hành ứng dụng SecureSMS

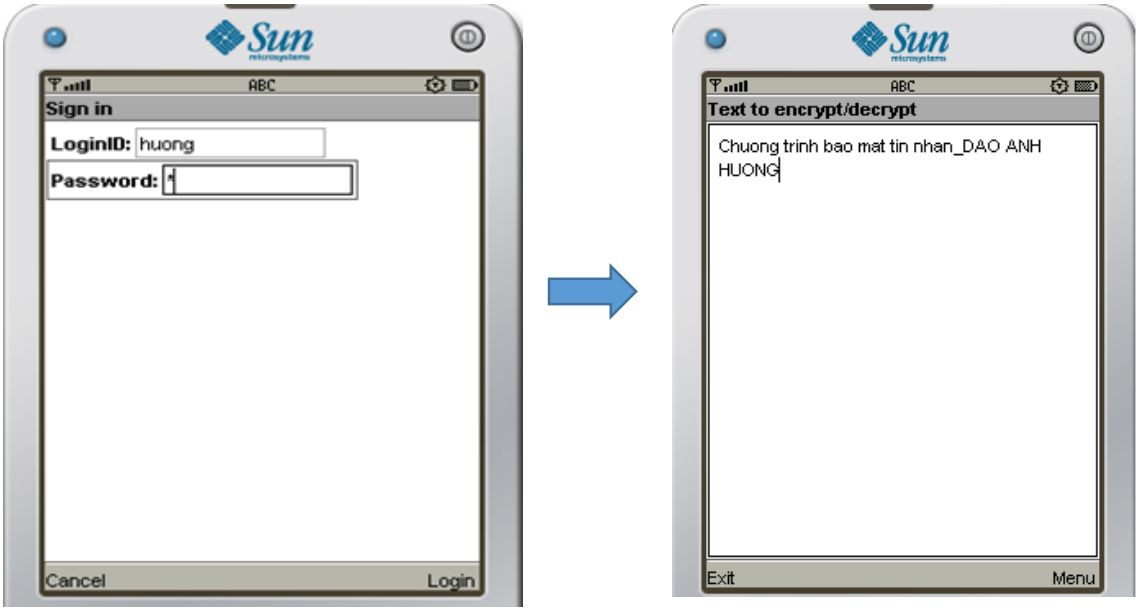
Khi đã mở dự án SecureSMS, ta kích nút Run ở chương trình để thi hành ứng dụng SecureSMS. Nếu chương trình mà chúng ta lập trình không có lỗi, một điện thoại mô phỏng được hiện ra với những tính năng đã được lập trình. Lúc này, chỉ cần nhấn phím Launch trên điện thoại mô phỏng để thực thi ứng dụng SecureSMS.

Hình 3.18: Thi hành ứng dụng SecureSMS bằng công cụ Wireless Toolkit

3.2.1.3. Đăng nhập chương trình SecureSMS

Tại đây, nhập tên tài khoản là “huong” và mật khẩu là “1” và sau đó nhấn Login để đăng nhập ứng dụng. Nếu đăng nhập thành công, chương trình SecureSMS sẽ mở ra với nội

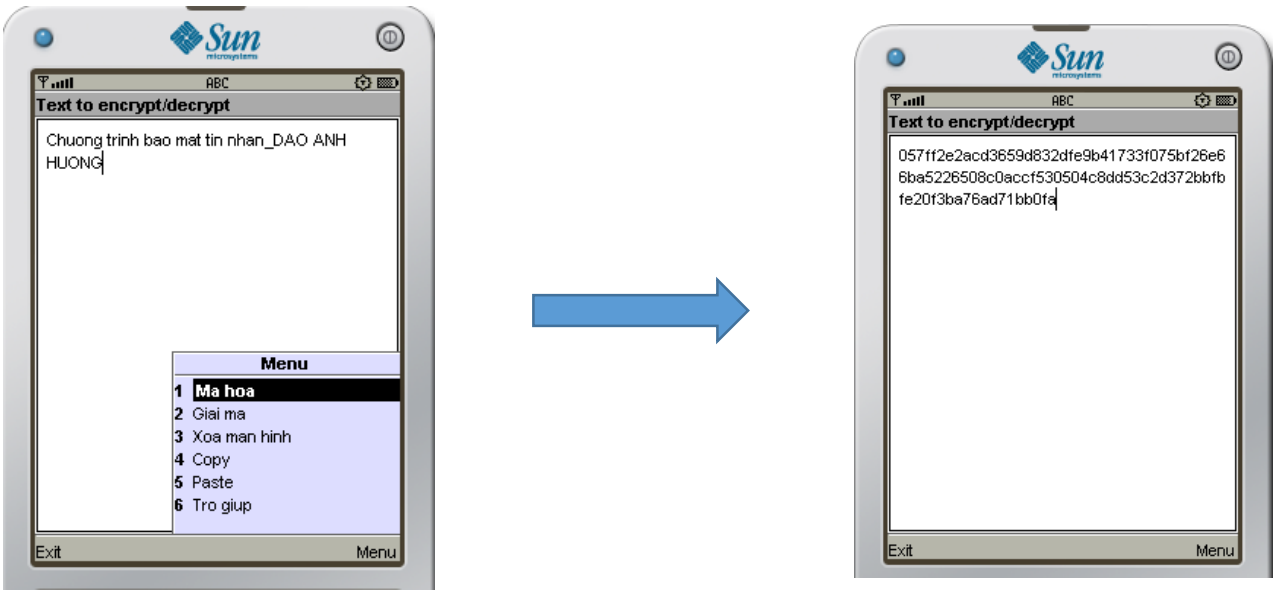
dung văn bản được khởi tạo bằng dòng chữ "Chuong trinh bao mat tin nhan_DAO ANH HUONG". Tại đây người dùng có thể sửa đổi nội dung theo ý muốn.



Hình 3.19: Đăng nhập vào chương trình SecureSMS ***Hình 3.20: Chương trình SecureSMS***

3.2.1.4. Các chức năng của chương trình SecureSMS

Để thực hiện các chức năng của chương trình, chỉ cần nhấn phím "Menu" trên điện thoại và chọn các chức năng muốn sử dụng. Giả sử, nếu muốn mã hóa một đoạn văn bản, chỉ cần soạn nội dung văn bản muốn mã hóa và chọn chức năng "Ma hoa" trong "Menu".



Hình 3.21: Các chức năng của chương trình SecureSMS ***Hình 3.22: Mã hóa văn bản***

Ngoài ra, chương trình SecureSMS còn vài chức năng khác như: Giải mã, xóa màn hình, copy, paste và chức năng trợ giúp.

3.2.2. Thử nghiệm chương trình trên điện thoại di động

Sau khi chương trình được thử nghiệm trên công cụ Wireless Toolkit thành công. Sử dụng chức năng đóng gói và obfuscation của công cụ đó để đóng gói chương trình SecureSMS thành tệp tin SecureSMS.jar. Sao chép tệp tin này vào máy điện thoại di động và cài đặt như một phần mềm bình thường.

KẾT LUẬN

Trong sự phát triển mạnh mẽ của công nghệ thông tin, cùng với nhu cầu cấp thiết về việc bảo vệ an ninh thông tin nói chung và bảo vệ thông tin cá nhân nói riêng, việc xây dựng các ứng dụng để bảo mật tin nhắn trên điện thoại di động là vô cùng quan trọng.

Trong phạm vi nghiên cứu, luận văn đã cơ bản giải quyết được yêu cầu đặt ra là "***Nghiên cứu phương pháp bảo mật tin nhắn trên điện thoại di động***":

- Nghiên cứu về lĩnh vực bảo mật tin nhắn trên ĐTDĐ cùng với các lỗ hổng bảo mật cũng như các giải pháp hiện nay đang áp dụng để bảo mật được tin nhắn;
- Nghiên cứu các phương pháp ứng dụng mã hóa để bảo mật tin nhắn;
- Xây dựng được chương trình demo bảo mật tin nhắn trên ĐTDĐ.

Tuy nhiên, do thời gian nghiên cứu và năng lực bản thân có hạn, tác giả mới chỉ xây dựng được chương trình demo bảo mật tin nhắn trên ĐTDĐ với những chức năng cơ bản và chương trình mới chỉ chạy được trên hệ điều hành Symbian, chưa chạy được trên hệ điều hành Android hay iOS…

**** Định hướng nghiên cứu và phát triển tiếp theo:***

Trong thời gian tới, tác giả sẽ tìm hiểu sâu thêm về các kỹ thuật, các giải pháp bảo mật tin nhắn trên điện thoại di động và bảo mật các thông tin trên điện thoại di động như là: danh bạ, tài liệu cá nhân, tranh ảnh…. Bên cạnh đó, tác giả sẽ nghiên cứu thêm để xây dựng phần mềm bảo mật thông tin trên điện thoại di động hoàn chỉnh, hiệu quả và có thể chạy trên nhiều hệ điều hành khác nhau.