NGHIÊN CỨU ỨNG DỤNG HỆ MẬT AES CHO HỆ THỐNG THÔNG TIN LIÊN LẠC ACARS TRONG NGÀNH HÀNG KHÔNG DÂN DỤNG

RESEARCH AND DEVELOPMENT OF AES CRYTOGRAPHY FOR ACARS SYSTEM IN CIVIL AVIATION

Hán Trọng Thanh, Phạm Thị Thương

*Viện Điện tử Viễn thông, Trường Đại học Bách Khoa Hà Nội*

*Email: thanh.hantrong@hust.edu.vn*

**Tóm tắt-** Hàng không dân dụng luôn là lĩnh vực cần phải đảm bảo tính an toàn gần như tuyệt đối. Trong các vấn đề đảm bảo an toàn bay, vấn đề đảm bảo an ninh an toàn thông tin liên lạc viễn thông trong quan lý không lưu là một trong những vấn đề quan trọng bậc nhất. Ngày nay, việc áp dụng các phương thức mã hóa thông tin hiện đại nhằm đảm bảo tính an toàn cho hệ thống thông tin viễn thông đã và đang được nghiên cứu, triển khai áp dụng trong nhiều lĩnh vực. Trong bài báo này, chúng tôi đề xuất triển khai hệ mật Advance Encryption Standard (AES) cho hệ thống thông tin liên lạc ACARS băng tần HF sử dụng trong ngành hàng không dân dụng. Các kết quả mô phỏng kênh truyền liên lạc HF đã được mã hóa sẽ được phân tích nhằm đánh giá hiệu năng hoạt động của hệ thống với phương pháp đề xuất.

**Từ khóa-** Quản lý không lưu; Hệ thống thông tin ACARS; Advance Encryption Standard; mã Turbo; Băng tần HF.

**Abstract-** In general, civil aviation is always required that it has to be the safetest field. One of the most important issues in ensuring flight safety is to guarantee the safety of communications systems which are used in Air Traffic Management. Nowadays, the application of Cryptography to ensure the safety of communications systems has been studied and implemented in many fileds. In this paper, we proposed a method to apply Advance Encryption Standard (AES) to the ACARS system with HF frequency band, which is used in the civil aviation. The simulation results of encoded messages on HF channel will be analyzed to evaluate the performance of proposed method.

**Key words-** Air Traffic Management (ATM); ACARS; AES; Turbo code; HF band.

1. **Đặt vấn đề**

Ngày nay, thông tin viễn thông băng tần HF ngày càng có vai trò quan trọng trong các hệ thống thông tin vô tuyến do tài nguyên tần số dần trở nên cạn kiệt so với nhu cầu sử dụng của con người. HF (High Frequency) có dải tần từ 3MHz cho đến 30 MHz, thuộc phổ tần vô tuyến hay còn được là vô tuyến sóng ngắn. Do đặc điểm lan truyền của HF trong khí quyển Trái Đất, vô tuyến sóng ngắn được sử dụng cho phát thanh, thông tin liên lạc tầm xa trong hàng hải và hàng không. Đặc biệt dùng HF có thể tiếp cận dễ dàng với các khu vực có địa hình hiểu trở như vùng núi, biển đảo… [[1](#Joh11)]

Năng lượng tần số vô tuyến sóng ngắn HF có khả năng tiếp cận bất kỳ vị trí nào trên Trái Đất vì nó có thể khúc xạ trở lại Trái Đất bởi tầng điện ly. Tầng điện ly được định nghĩa là vùng khí quyển bắt đầu ở độ cao khoảng 60-70 km tính từ bề mặt Trái Đất và kéo dài đến khoảng hơn 1000 km. Tính chất đặc trưng của tầng điện ly là có độ dẫn điện cao do các thành phần không khí ở đây bị bức xạ mặt trời ion hóa, tạo ra một môi trường khí quyển có khả năng dẫn điện, khúc xạ sóng HF và cho phép thực hiện truyền sóng với khoảng cách rất xa. Thông tin liên lạc sử dụng băng tần HF có ưu điểm nổi bật là đơn giản, dễ di động, chi phí thấp, hiệu quả cao và đặc biệt là không phụ thuộc vào nhà cung cấp dịch vụ như thông tin vệ tinh [[2](#Bin11)]. So với các loại hình khác thì thông tin liên lạc sóng ngắn HF là một sự lựa chọn tốt nhất, có những ưu điểm vượt trội.

Trong những năm gần đây, vấn đề an toàn an ninh thông tin hàng không đã và đang bị đe dọa bởi các nguy cơ như khủng bố cũng như các thế lực thù địch ở cả trong và ngoài nước. Chính vì lý do đó, việc đảm bảo an toàn các hệ thống thông tin liên lạc cho ngành hàng không luôn được các cơ quan chức năng cũng như các nhà khoa học quan tâm nghiên cứu, triển khai và áp dụng.

|  |
| --- |
|  |
| ***Hình 1.*** *Mô hình các đường truyền thông tin giữa máy bay và trạm mặt đất* |

Một trong những hệ thống thông tin viễn thông điển hình sử dụng trong ngành hàng không là hệ thống ACARS (Aircraft Communications Addressing and Reporting System). Đây là hệ thống liên lạc dữ liệu số cho phép truyền tải các dữ liệu, bản tin ngắn cần thiết giữa máy bay và các trạm mặt đất thông qua sóng vô tuyến hoặc vệ tinh [3][4]. Giao thức trao đổi của hệ thống do công ty ARINC (Aeronautical Radio, Mỹ) thiết kế với mục đích để thay thế các dịch vụ thoại qua tần số VHF trước đây. Thông thường, hệ thống ACARS sẽ sử dụng bộ phát đáp VHF số 3 trên máy bay (thường có 3 bộ phát đáp VHF, 2 bộ HF và 1 bộ AM) . Khối điều khiển sẽ thực hiện mã hóa dữ liệu số cần truyền thành chuỗi hai âm 1.200 Hz và 2.400 Hz với tốc độ chỉ 2.400 baud. Các hệ thống mới có thể hỗ trợ và hoạt động với 2.400/4.800Hz với tốc độ 4.800 baud. Các bộ thu phát vô tuyến HF/VHF có thể dùng cho tín hiệu đàm thoại của phi hành đoàn hoặc cho các chức năng khác. Do đó, bộ điều khiển ACARS sẽ có một số mode hoạt động chủ động hoặc theo trạng thái chờ. Khi bộ thu phát vô tuyến “rảnh”, hệ thống sẽ tự động thực hiện trao đổi số liệu với mặt đất để cập nhật thông tin [5].

Trong quá trình thông tin liên lạc giữa máy bay và trung tâm quản lý không lưu dưới mặt đất, các lực lượng không được phép như khủng bố, các thế lực thù địch trong nước và nước ngoài hoàn toàn có thể nghe lén để biết lịch trình bay cũng như nhiều thông tin khác liên quan đến chuyến bay. Điều này có thể dẫn tới những sự việc có thể uy hiếp an toàn chuyến bay nói riêng cũng như an toàn hàng không nói chung. Chính vì lý do đó, việc tăng cường tính bảo mật cho thông tin liên lạc hàng không qua các kênh vô tuyến là cấp thiết. Đã có một số công trình nghiên cứu trong và ngoài nước về vấn đề bảo mật thông tin thoại và số liệu cho liên lạc hàng không. Tuy nhiên, đây là những nghiên cứu chỉ cho lĩnh vực quân sự mà chưa có những ứng dụng cho ngành hàng không dân dụng [6]. Trong bài báo này, nhóm nghiên cứu tiến hành nghiên cứu các chuẩn bảo mật thông tin và đề xuất áp dụng chuẩn bảo mật Advance Encryption Standard cho hệ thống thông tin ACARS băng tần HF cho ngành hàng không dân dụng. Bài báo bao gồm các phần như sau.

* Phần 1 – Đặt vấn đề.
* Phần 2 – Giới thiệu chuẩn bảo mật AES, phần này sẽ giới thiệu sơ lược về chuẩn bảo mật AES, các thành phần cấu trúc của chuẩn này.
* Phần 3 – Kết quả mô phỏng.
* Phần 4 – Kết luận

1. **Chuẩn bảo mật AES**

## Giới thiệu chung về chuẩn bảo mật AES

Tiêu chuẩn Advanced Encryption Standard (AES) – Chuẩn mã hóa tiên tiến là một thuật toán tiêu chuẩn của chính phủ Hoa Kỳ nhằm mã hóa và giải mã dữ liệu do Viện Tiêu chuẩn và Công nghệ quốc gia Hoa Kỳ (NIST) phát hành ngày 26/11/2001 và được đặc tả trong Tiêu chuẩn Xử lý thông tin Liên bang 197 (FIPS 197). AES là một thuật toán “mã hóa khối” (block cipher) ban đầu được tạo ra bởi hai nhà mật mã học người Bỉ là Joan Daemen và Vincent Rijmen, cho phép xử lý các khối dữ liệu đầu vào có kích thước 128 bit sử dụng các khóa có độ dài 128, 192 hoặc 256 bit. [7]

Các tổ hợp khóa – khối – vòng phù hợp đối với tiêu chuẩn này thể hiện trong bảng sau:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Độ dài khóa  (Nk) | Độ dài khối  (Nb) | Số vòng  (Nr) |
| AES - 128 | 4 | 4 | 10 |
| AES - 192 | 6 | 4 | 12 |
| AES - 256 | 8 | 4 | 14 |

Quá trình mật mã hóa và giải mã của hệ mật AES được thể hiện qua hình vẽ sau:

|  |
| --- |
|  |
| ***Hình 2.*** *Quá trình mật mã hóa (Encryption) và giải mã (Decryption) của hệ mật AES* |

* 1. ***Quy trình mã hóa và giải mã của hệ mật AES***

Quy trình mã hóa sử dụng bốn phép biến đổi chính như sau:

* ***AddRoundKey:*** cộng modulo mã khóa của chu kỳ vào trạng thái hiện hành. Độ dài của mã khóa của chu kỳ bằng với kích thước của trạng thái.
* ***SubBytes:*** thay thế phi tuyến mỗi byte trong trạng thái hiện hành thông qua bảng thay thế (SBox).
* ***MixColumns:*** trộn thông tin của từng cột trong trạng thái hiện hành. Mỗi cột được xử lý độc lập.
* ***ShiftRows***: dịch chuyển xoay vòng từng dòng của trạng thái hiện hành với số bước dịch khác nhau.

|  |
| --- |
|  |
| Mật mã (Encryption) Giải mật mã(Decryption)  ***Hình 3.*** *Cấu trúc của một vòng mật mã hóa* |

Trong hệ mật AES, bản tin rõ cần truyền sẽ được mã hóa qua rất nhiều vòng mã hóa như mô tả ở hình 3. Mỗi vòng mã hóa sẽ thực hiện lần lượt các phép biến đổi với thứ tự như sau: bản tin cần truyền sẽ được xử lý với thao tác AddRoundKey đầu tiên trước khi thực hiện các chu kỳ mã hóa. Trong quá trình mã hóa sẽ có chu kỳ mã hóa. Bình thường, mỗi chu kỳ bao gồm bốn bước biến đổi liên tiếp nhau: SubBytes, ShiftRows, MixColumns, và AddRoundKey. Có một điểm đáng lưu ý đó là trong chu kỳ cuối cùng phép biến đổi MixColumns sẽ bị lược bớt đối với quá trình mật mã hóa và tương ứng với phép InvMixcolumns đối với quá trình giải mật mã hóa. Các phép biến đổi nêu trên có vai trò biến đổi bản tin rõ cần gửi dễ bị đọc trộm hay nghe lén để trở thành bản tin mật có độ phức tạp rất cao. Chi tiết về các phép biến đổi đó như sau.

|  |
| --- |
|  |
| ***Hình 4.*** *Mô hình hóa biến đổi SubBytes – InvSubBytes thông qua bảng Sbox – Sbox-1* |

***SubBytes – InvSubBytes***: đây là bước thay thế phi tuyến mỗi byte trong trạng thái hiện hành thông qua bảng thay thế (SBox) đối với quá trình mật mã hóa, SBox-1 đối với giải mã hóa.

***ShiftRows – InvShiftRows:*** các bước thực hiện của quá trình dịch chuyển xoay vòng từng dòng của các trạng thái hiện hành như sau:

* Mỗi dòng của trạng thái hiện hành được dịch chuyển xoay vòng đi một số vị trí.
* Byte tại dòng cột sẽ dịch chuyển đến cột.
* Phép biến đổi ngược InvShiftRows: Byte tại dòng cột sẽ dịch chuyển đến cột .

|  |
| --- |
|  |
| ***Hình 5.*** *Mô hình hóa biến ShiftRows - InvShiftRows* |

***MixColumn – InvMixColumn:*** xáo trộn thông tin của từng cột trong mỗi một trạng thái riêng biệt với phương thức như sau:

* Mỗi cột của trạng thái hiện hành được biểu diễn dưới dạng đa thức có các hệ số trên trường .
* Thực hiện phép nhân:

|  |  |
| --- | --- |
|  | (1) |

với

* Đối với quá trình InvMixcolumn, quá trình thực hiện phép toán ngược:

|  |  |
| --- | --- |
|  | (2) |

với

|  |
| --- |
|  |
| ***Hình 6.*** *Mô hình biến đổi MixColumn - InvMixColumn* |

***AddRoundKey:*** là phép thực hiện phép toán XOR Key của từng Round với State sinh ra sau phép biến đổi MixColumn đối với quá trình mật mã hóa và sau phép InvSubBytes đối với quá trình giải mật mã hóa.

|  |
| --- |
|  |
| ***Hình 7.*** *Mô hình biến đổi AddRoundKey* |

Ngoài 4 phép biến đổi nêu trên, một tiến trình khác rất quan trọng đối với hệ mật AES cần phải nhắc đến đó là tiến trình tạo khóa (KEY) cho mỗi vòng mã hóa. Tiến trình này được mô tả như trên hình vẽ sau.

|  |
| --- |
|  |
| ***Hình 8.*** *Mô hình mã hóa chu kỳ với độ dài mã khóa chính 128 bit* |

* Với 4 *words* (w) đầu tiên được tạo ra từ khóa mật mã (Cipher key – là mảng 16 bytes *k0÷k15*).
* Phần còn lại, wi (i= 3÷43) được tạo ra như sau:
  + Nếu
  + Nếu thì .

Với [9].

1. **Thiết kế hệ thống và mô phỏng đánh giá**

Trong phần này, chúng tôi đề xuất giải pháp tăng tính bảo mật cho hệ thống truyền dữ liệu qua băng tần HF của hệ thống ACARS cho ngành hàng không dân dụng. Hệ thống được xây dựng và mô phỏng bằng ngôn ngữ lập trình Matlab với sơ đồ như hình vẽ sau.

|  |
| --- |
|  |
| ***Hình 9.*** *Sơ đồ khối thu phát dữ diệu với kênh truyền HF* |

Trong đó

* Khối Source data dưới dạng text, ta tiến hành chuyển về chuỗi bit và chia thành các khối 128 bit theo chuẩn đầu vào của AES để truyền.
* Khối AES Encryption nhận đầu vào là khối bit vừa được biến đổi ở trên cùng khóa Key được nhập, sau đó tiến hành mật mã hóa bằng hệ mật AES.
* Khối Channel encoding/decoding: Kênh truyền được mã hóa theo mã Turbo.
* Khối điều chế/giải điều chế: 16-QAM
* Khối HF Channel: Kênh truyền HF được giả sử chỉ có nhiễu AWGN (Additive White Gaussian Noise)

Giao diện phần mềm mô phỏng truyền và nhận dữ liệu qua kênh truyền HF đã được xây dựng như sau.

|  |
| --- |
|  |
| ***Hình 10.*** *Giao diện Transmitter/Receiver truyền text* |

Với các thông số đã quy định ở phần trên, nhóm nghiên cứu tiến hành chạy mô phỏng chương trình với:

* Bản tin rõ cần gửi có nội dung: “ASELAB - Bo mon ky thuat dien tu hang khong vu tru - Vien Dien Tu vien thong – Dai hoc Bach Khoa Ha Noi” (dung lượng 106 Byte).

Với khóa mật mã – Key: “*ABCDEF123456789ABCDEF123456789ABCDEF123456789ABCDEF123456789ABCD*”

Bản tin mật sau khi mã hóa nhận được có nội dung là: “*î«­ÄI!x©îçÁUÄæç¹8¦Ñ!Y¥´ã"zþÿt|à×h 3A÷Ä|Àþø²mi3²á÷Ùtè5²SúØaëcgõ<vÑÄÂ¤7¸Uiúx ®z =á•Ø6å3 ´!5O*”. Rõ ràng, với bản mật như vậy, dù có nghe lén thì trong thời gian ngắn đối phương cũng chưa thể giải mã được bản tin do tính bảo mật rất cao của hệ mật AES [9]. Mặt khác, với kênh truyền vô tuyến HF được mã hóa theo mã Turbo trong điều kiện bị ảnh hưởng bởi nhiễu trắng, tỉ lệ lỗi bit qua mô phỏng khảo sát được thể hiện trong hình sau.

|  |
| --- |
|  |
| ***Hình 11.*** *Đồ thị tỉ lệ lỗi bit khi thực hiện truyền text với hệ mật AES 256 bit* |

Như vậy, bằng việc mô phỏng đề xuất áp dụng hệ mật AES cho truyền dữ liệu qua kênh truyền vô tuyến bằng HF chúng ta nhận thấy nội dung đoạn text thu được khá chính xác, tỉ lệ lỗi bit BER thấp, do đó việc áp dụng hệ mật mã AES 256 bit là khả thi.

1. **Kết luận và hướng nghiên cứu tiếp theo**

Qua bài báo này, chúng tôi đã đề xuất việc triển khai hệ mật AES trong việc truyền thông dữ liệu của hệ thống ACARS băng tần HF. Điều này sẽ tăng tính bảo mật cho hệ thống, ngăn chặn việc nghe lén thông tin cũng như giảm thiểu các nguy cơ xảy ra uy hiếp sự an toàn của ngành hàng không. Mặt khác, chúng ta thấy rằng việc chèn thêm hệ mật dữ liệu không hề làm ảnh hưởng đến hiệu quả làm việc của hệ thống như thời gian xử lý, tốc độ bit hay tỉ lệ lỗi bit... Do đó, đề xuất này là có tính khả thi trong thực tế.

Trong thời gian tới, chúng tôi sẽ tiếp tục nghiên cứu các phương thức mã hóa khác cùng các phương thức triển khai các hệ mật đó đối với hệ thống thông tin thoại được sử dụng trong ngành hàng không dân dụng Việt Nam cũng như các hệ thống thông tin viễn thông vô tuyến khác.

**TÀI LIỆU THAM KHẢO**

[1] John Martin Wilson, "A Low Power HF Communication System," Ph.D thesis, School of Electrical and Electronic Engineering, The University of Manchester, 2011.

[2] Manikant Yadav Bindu Mangla, "Chemistry of Upper Ionosphere-A Study ," *International Journal of Advances in Engineering Sciences* , no. 1, p. 4, Jan. 2011.

[3] Secure aircraft communications addressing and reporting system (ACARS) Roy, A.; Digital Avionics Systems, 2001. DASC. The 20th Conference, vol.:2, pp.: 7A2/1-7A2/11, Oct. 14-18, 2001.

[4] Moninger, William R., and Patricia A. Miller. "FA 1A. 2 ACARS QUALITY CONTROL, MONITORING, AND CORRECTION." (1994).

[5] Nguyễn Khánh Tiềm, “ACARS - Hệ thống thông tin và báo cáo hỗ trợ cho phi công trên máy bay dân dụng”, *Tạp chí Công nghệ thông tin và truyền thông*, p.4, 03/2014.

[6] Lưu Tuấn Sinh, "Nghiên cứu giải pháp công nghệ, thiết kế lắp đặt hệ thống thông tin tác chiến giữa các đảo ở quần đảo Trường Sa", Viện kỹ thuật Hải Quân, 2010.

[7] Federal Information Processing Standards Publication 197: National Institute of Standards and Technology (NIST), November 26, 2001.

[8] V. K. PACHGHARE, CRYPTOGRAPHY AND INFORMATION SECURITY, 2nd ed.: PHI Learning Pvt. Ltd., 2015, 2015.

[9] Adi Shamir, Eran Tromer Dag Arne Osvik, Cache Attacks and Countermeasures: the Case of AES. Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot 76100, Israel, 20/11/2005.

**Thông tin liên lạc:**

**TS. Hán Trọng Thanh**

Tên cơ quan:  Viện Điện tử viễn thông, ĐH Bách Khoa Hà nội

Email: thanh.hantrong@hust.edu.vn

(BBT nhận bài: …/…/2016, phản biện xong: …/…/2016)