Chapter 04B: Message Authetication Codes(MAC)

Message authentication là 1 cơ chế hoặc dịch vụ được sử dụng để xác minh tính toàn vẹn của thông điệp.

Xác định dữ liệu không bi sửa đổi, xóa hoặc replay và danh tính người gửi là xác thực.

MAC là một thuật toán mà yêu cầu sử dụng 1 khóa bí mật. một MAC có một thông điệp có độ dài biến đổi và một khóa bí mật như là đầu vào và tạo ra mã xác thực.

Một cách: một MAC kết hợp một hàm băm trong 1 số trường hợp với 1 khóa bí mật.

Cách khác: sử dụng mã hóa khối đối xứng trong 1 cách mà nó tạo ra output có độ dài cố định từ input độ dài biến đổi.

**Message Authentication Requirements:**

Disclosure: phát hành nội dung tin nhắn cho bất kỳ người nào hoặc quá trình không sở hữu chìa khóa mã hóa thích hợp.

Traffic analysis: phát hiện mô hình lưu lượng giữa các bên.

Masquerade: đầu vào của tin nhắn từ 1 nguồn gian lận.

Content modification: Những thay đổi nội dung của một tin nhắn, bao gồm chèn, xóa, chuyển vị, và sửa đổi.

Sequence modification: Bất kỳ sửa đổi cho một chuỗi các thông điệp giữa các bên, bao gồm chèn, xóa, và sắp xếp lại.

Timing modification: Delay hoặc phát lại các tin nhắn.

Source repudiation: nguồn thoái thoát.

Destination repudiation: đích thoái thoát.

MAC : đảm bảo message từ nguồn không bị sửa đổi; xác thực trình tự và thời hạn;chữ ký số đảm bảo chống chối bỏ từ nguồn và đích.

|  |  |
| --- | --- |
| Hash function: | Message authentication code (MAC) |
| Một chức năng mà ánh xạ một tin nhắn có độ dài bất kỳ thành một giá trị hash độ dài dài cố định phục vụ như là xác thực. | Một function của thông điệp và một khóa bí mật tạo ra một value độ dài cố định phục vụ như là xác thực. |

**Brute-Force Attacks(Two lines of attack):**

**Attack the key space**

•If an attacker can determine the MAC key then it is possible to generate a valid MAC value for any input x

**Attack the MAC value**

• Objective is to generate a valid tag for a given message or to find a message that matches a given tag.

**Cryptanalysis**

Cryptanalytic attacks seek to exploit some property of the algorithm to perform some attack other than an exhaustive search.

An ideal MAC algorithm will require a cryptanalytic **effort greater than** or equal to the brute-force effort.

There is much more variety in the structure of MACs than in hash functions, so it is **difficult to generalize about the cryptanalysis of MACs**.