**Chương 2 : Cryptography ( hệ thống mật mã )**

* giao thức IPSec
* giao thức PGP
* giao thức SSL

**Main terms used in cryptography**

* Plaintext :
* Encryption algorithm ( thuật toán mã hoá ) :
* Secret key :
* Ciphertext ( có thể trao đổi an toàn ) :
* Decryption algorithm ( thuật toán giải mã ) :

**How does it work ?**

**Mô hình mã hoá đối xứng** ( chìa khoá mã hoá cũng là chìa khoá giải mã )

Plaintext 🡪 encryption 🡪 ciphertext 🡪 decryption 🡪 plaintext

**Break a cipher**

Tấn công dạng buteforce : Thử mọi trường hợp có thể xảy ra để có thể giải.

Tấn công phi kỹ thuật ( sử dụng kỹ thuật về xã hội ) : mạo danh, giả danh, lừa người dùng

**Cần quan tâm 2 đối tượng** **( Brute – Force attack and Cryptanalysis )**

Brute-force attack : đại diện nhóm người mũ đen

Cryptanalysis : đại diện nhóm người mũ trắng

**Cipher Strength ( đánh giá thuật toán mã hoá )**

* **The cost** of breaking the cipher exceeds the value of encrypted information ( low value ) ( giá trị của thông tin mã )
* **The time** required to break the cipher exceeds the useful lifetime of the information ( large time ) ( thời gian giải mã )

**Thời gian trung bình yêu cầu tìm các key :**

* Kích thước của key ( bits )
* Number of alternative keys
* Time required at 1 Decryption/ micro giây
* Tỉm required at 10 mũ 6 Decryption / micro giây

**Cryptography :**

* Đòi hỏi tính xác thực
* Đảm bảo nguồn gốc của thông điệp ( tính chịu trách nhiệm )

**Taxonomy of Cryptography :**

Có 3 nhóm :

**The type of operations used for transforming plaintext to ciphertext :**

**Substitution ( thay thế** : thay kí tự này thành ký tự khác ) – key mã hoá cũng là key giải mã.

* Caesar : thay thế kí tự bằng chữ bảng chữ cái tiếng anh, thay ký tự bằng chữ cái nằm bên phải ký tự cách k đơn vị hoặc có những thuật toán khác nhau để thay thế.
* Monoalphabetic ciphers ( tốt hơn Caesar ) :
  + Thống kê tần số xuất hiện kí tự. Easy to break by brute force because they reflect the **frecquency data** of the original alphabet.
  + Dựa vào tần số xuất hiện của ký tự mà thay thế ký tự đó vào dựa theo tần số tương ứng.
* Playfair cipher :
  + Ví dụ : cho 1 từ : Hellos . Keyword là MONARCHY. Tạo bảng playfair : tạo bảng 5x5, viết keyword vào, sau đó viết các chữ cái trong bảng chữ cái tiếng anh, chữ nào trùng với ký tự của keyword thì bỏ qua, I và J nằm chung ô.

A white grid with letters and a cursor

Description automatically generated

Xét từ cần mã hoá, lấy từng cặp ký tự để xét :

* + HB cùng hàng 🡪 thay bằng ký tự cùng hàng bên phải của từng ký tự nên ta được YD
  + HV cùng cột 🡪 thay bằng ký tự cùng dòng bên trên của từng ký tự nên ta được OP. Nếu ký tự không có ký tự ở trên nữa, thì lấy vòng xuống dưới cùng. Ví dụ : O thì sẽ lấy V
  + HS không cùng hàng, không cùng cột 🡪 lấy ký tự ở điểm giao nhau giữa hàng và cột chứa 2 ký tự này ( tạo thành hình chữ nhật ) ta được BP
  + Nếu có 2 ký tự trùng ( giống nhau ) thì xem như cùng hàng, cùng cột 🡪 lấy bên trái và dịch lên 1 ô.
  + Bài tập :
    - C= Fuvvnxsmunvtamxasuoitt, K=security

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| FU | VV | NX | SM | UN | VT | AM | XA | SU | OI | TT |
|  |  |  |  |  |  |  |  |  |  |  |
| HE | LL | OW | EL | CO | ME | TO | OU | RC | LA | SS |
|  |  |  |  |  |  |  |  |  |  |  |
| Hello | welcome | to | our | class |  |  |  |  |  |  |

* Vigenere Cipher :
  + Bảng Vigenere Cipher

A screenshot of a game

Description automatically generated

**Transpotion ( thay đổi vị trí )**

* Rail fence ( đơn giản nhất ) :
* Transposition technique : chia độ dài cipher text cho độ dài của key …

**Sysmetric & Asymmetric Encryption**

* Public key : có thể cho người khác biết, dùng để mã hoá thông điệp, check the signature of key’s owner.
* Private key : chỉ người tạo biết, dùng để giải mã thông điệp, create the signature.

Public for encryption, private for decryption.

Private for signing, public for verification.

**Asymmetric Encryption with private key**

Authenitication and signature

**Hash Functions ( hàm băm – hàm hash )**

**h = H(M)**

* Biến đổi đầu vào thành đầu ra khác biệt.
* Không có thuật toán giải mã ngược lại. Chỉ còn cách thử từng cái.