
KSTP.Ebook

CHƯƠNG I
LÝ THUYẾT THÔNG TIN TRONG CÁC HỆ MẬT

Giới thiệu môn học

- Nội dung
  - Chương 1: Nhập môn mật mã học
  - Chương 2: Mật mã khoá bí mật
  - Chương 3: Mật mã khoá công khai
  - Chương 4: Hàm băm, xác thực và chữ kí số

Giới thiệu môn học

- Thời lượng
  - 60 tiết = 4 đơn vị học trình
- Hình thức thi và kiểm tra
  - Thi viết
  - Sau các bài có thể có bài tập về nhà hoặc có các hình thức kiểm tra

Nội dung chính

- 1.1 Một số khái niệm cơ bản trong mật mã
- 1.2 Sơ đồ khối đơn giản của một HT thông tin số
- 1.3 Thuật toán và độ phức tạp
  - 1.3.1 Khái niệm về thuật toán
  - 1.3.2 Độ phức tạp của thuật toán
- 1.4 Độ mật hoàn thiện
  - 1.4.1 Quan điểm về độ an toàn của hệ mật
  - 1.4.2 Nhắc lại một số lí thuyết cơ bản về xác suất
  - 1.4.3 Độ mật hoàn thiện
- 1.5 Entropy
- 1.6 Các khóa giả và khoảng duy nhất

1.1 Một số khái niệm cơ bản

- Bản rõ (Plaintext): Dạng ban đầu của thông báo
- Bản mã (Ciphertext): Dạng mã của bản rõ ban đầu
- Khóa (Key): thông tin tham số dùng để mã hóa.
- Mã hóa (Encryption): Quá trình mã 1 thông báo sao cho nghĩa của nó không bị lộ ra
- Giải mã (Decryption): Quá trình ngược lại biến đổi 1 thông báo đã mã ngược trở lại thành dạng thông thường.

1.1 Một số khái niệm cơ bản

- Kí hiệu:
  - $y = E_k(x)$: y là bản mã của bản rõ x qua hàm biến đổi E (hàm mã hóa) với khóa K
  - $x = D_k(y)$: x là bản rõ của bản mã y qua hàm biến đổi D (hàm giải mã) với khóa K

1.1 Một số khái niệm cơ bản

- Ví dụ minh họa:
  - Bản rõ x: HELLOWORLD
  - Hàm $e_k(x) = x + k \bmod 26$
  - Cho k = 5

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

  - Khi đó: bản mã $y = e_k(x)$ = MJRRTBTWRI
    - H: $7 + 5 \bmod 26 = 12 \leftrightarrow$ M;
    - E: $4 + 5 \bmod 26 = 9 \leftrightarrow$ J;
    - …
  - Ta cũng có thể suy ra bản rõ x từ bản mã y từ hàm giải mã:

$$d_k(y) = y - k \bmod 26$$

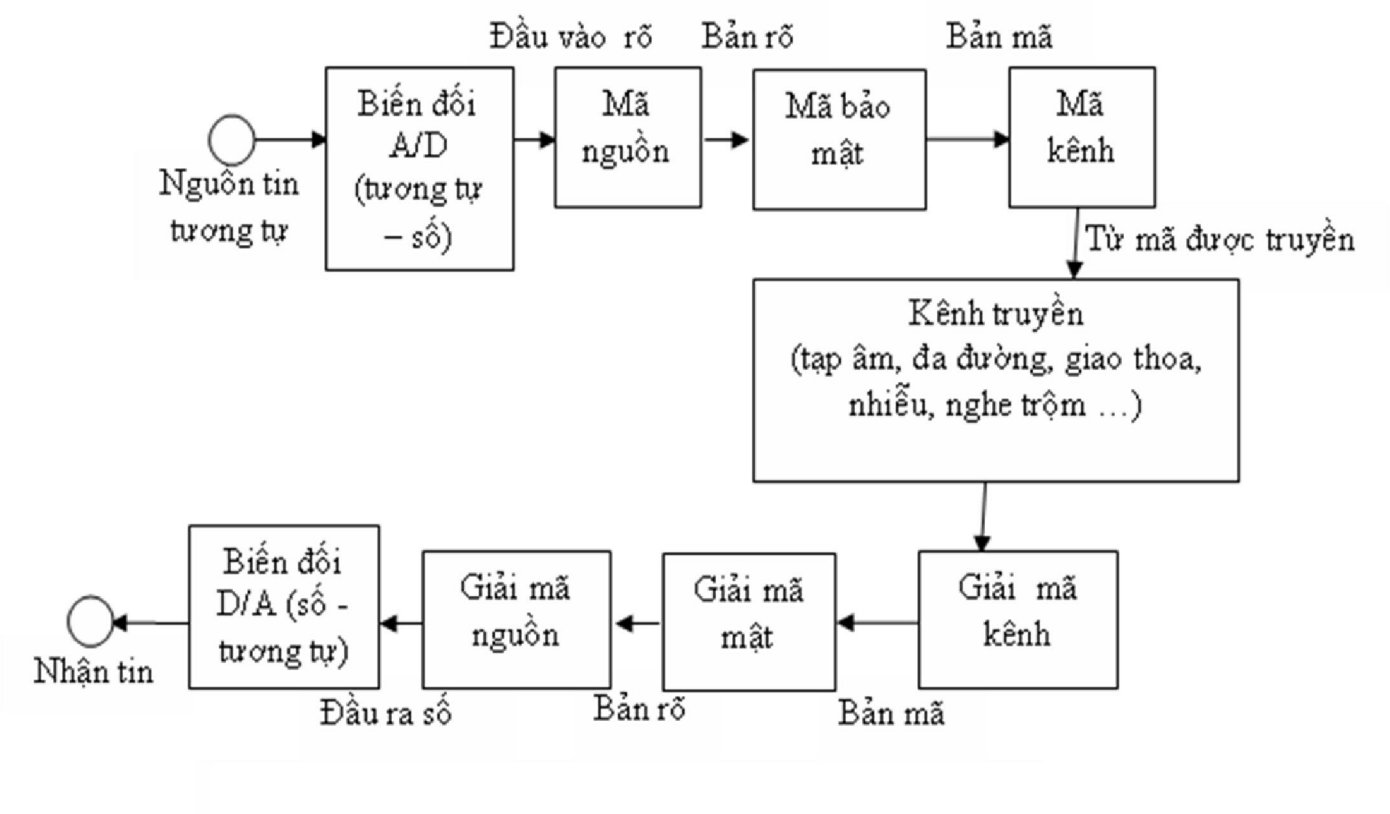
1.1 Một số khái niệm cơ bản

- Khoa học mật mã (cryptology) gồm:
  - Mật mã học (cryptography): là khoa học nghiên cứu cách ghi bí mật thông tin nhằm biến đổi bản rõ thành bản mã.
  - Phân tích mật mã (cryptanalysis): nghiên cứu cách phá các hệ mật nhằm phục hồi bản rõ ban đầu từ bản mã, nghiên cứu các nguyên lí và phương pháp giải mã mà không biết khóa.
    - Có 3 phương pháp tấn công cơ bản của thám mã:
      - Tìm khóa vét cạn
      - Phân tích thống kê
      - Phân tích toán học

1.1 Một số khái niệm cơ bản

- Các kiểu tấn công thám mã:
  - Tấn công chỉ với bản mã: biết thuật toán, bản mã, dùng phương pháp thống kê xác định bản rõ
  - Tấn công với bản rõ đã biết: biết thuật toán, biết được bản mã/bản rõ, tấn công tìm khóa
  - Tấn công với các bản rõ được chọn: chọn bản rõ và nhận được bản mã, biết thuật toán, tấn công tìm khóa.
  - Tấn công với các bản mã được chọn: chọn bản mã và có được bản rõ tương ứng, biết thuật toán, tấn công tìm khóa.
- Chú ý:
  - Hệ mật có thể bị phá chỉ với bản mã thường là hệ mật có độ an toàn thấp
  - Hệ mật là an toàn với kiểu tấn công có các bản rõ được chọn thường là hệ mật có độ an toàn cao

1.2 Sơ đồ khối đơn giản của một HTTTS



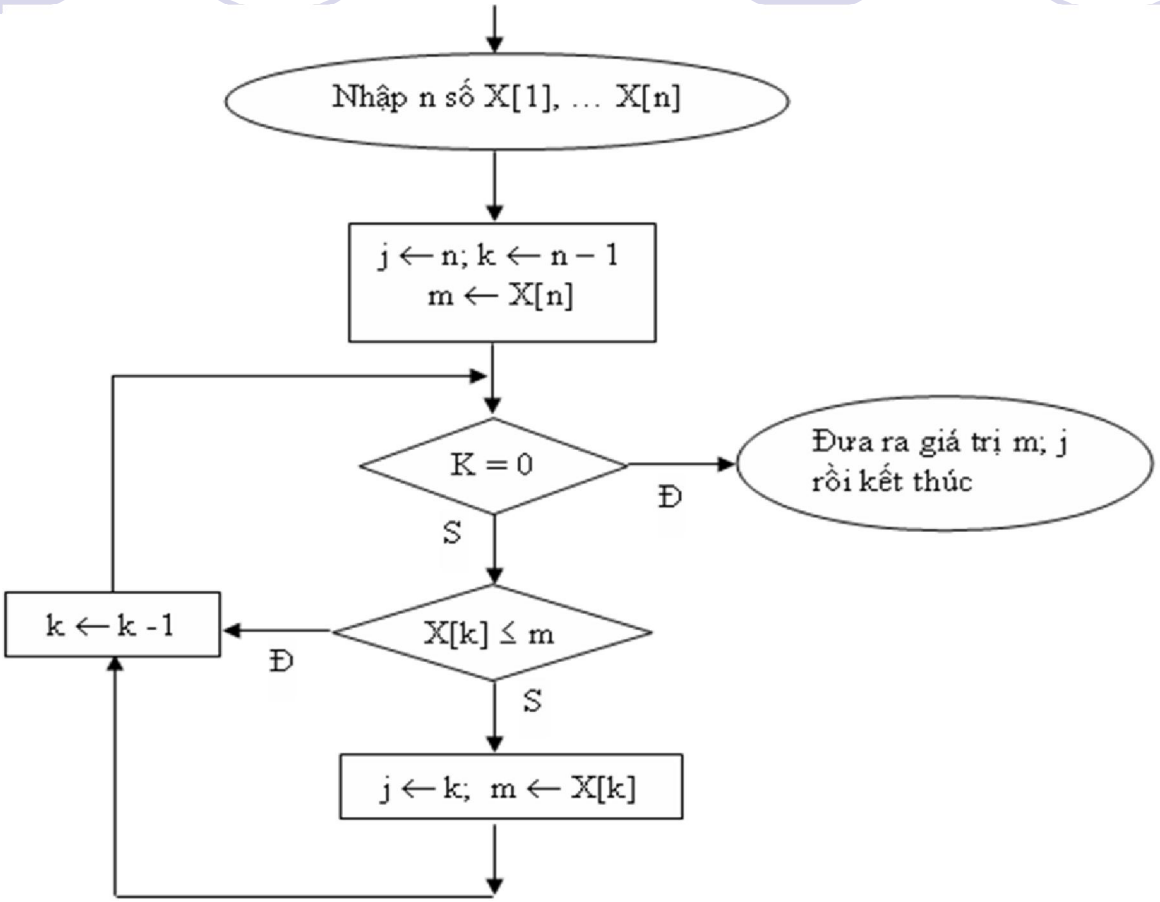
1.2. Sơ đồ khối…

- Qua sơ đồ của HTTTS, ta thấy được ý nghĩa của khối mã bảo mật đó là bảo vệ các thông tin không bị khai thác bất hợp pháp. Chống lại các tấn công sau:
  - Thám mã thụ động: là cách do thám, theo dõi đường truyền để nhận được nội dung bản tin hoặc theo dõi luồng truyền tin. Bao gồm các hoạt động: thu chặn, dò tìm, so sánh tương quan, suy diễn.
  - Thám mã tích cực (chủ động): thay đổi dữ liệu để giả mạo một người nào đó, lặp lại bản tin trước, thay đổi bản tin khi truyền, từ chối dịch vụ. Bao gồm các hoạt động: giả mạo, ngụy trang, sử dụng lại, sửa đổi.

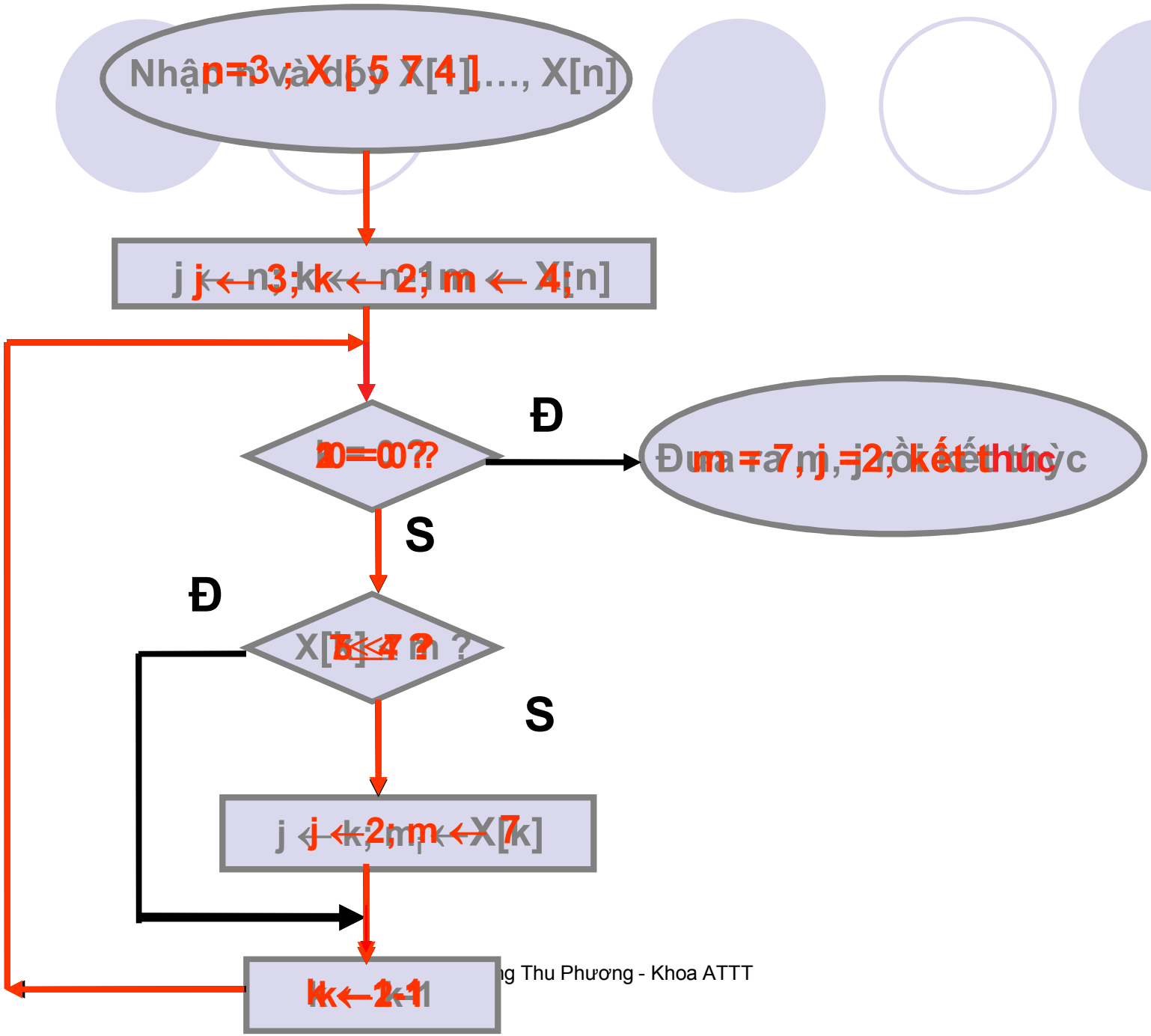
1.3. Thuật toán và độ phức tạp

- 1.3.1 Khái niệm: Thuật toán là một quy tắc để với những dữ liệu ban đầu đã cho, tìm được lời giải của bài toán được xét sau một số bước thực hiện.
  - VD: Thuật toán tìm cực đại
    - Input: cho n số X[1],…, X[n]
    - Output: m, j sao cho $m = X[j] = \max_{1 \le k \le n} X[k]$

1.3. Thuật toán …



Sơ đồ khối của thuật toán tìm cực đại

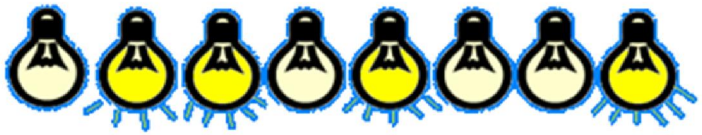

Nhập n và dãy X[1], X[2], …, X[n]
j ← n; k ← n-1; m ← X[n]
j = 0 ??
Đ
Đưa ra m, j, rồi kết thúc
S
Đ
X[k] < m ?
S
j ← k; m ← X[k]
k ← k-1

1.3. Thuật toán …

- Nhận xét:
  - Thuật toán có tính hữu hạn
  - Thuật toán có tính xác định

1.3. Thuật toán …

- 1.3.2 Độ phức tạp của thuật toán
  - Trong khi làm việc MT thường ghi các số bằng bóng đèn sáng tắt. Quy ước: bóng đèn sáng chỉ số 1; bóng đèn tắt chỉ số 0
    - VD: dãy bóng đèn tắt sáng sau:



biểu thị cho dãy bít: **01101001**

  - Độ phức tạp của thuật toán được đo bằng số các phép tính bít (phép tính logic, số học) thực hiện trên các bit 0 và 1.
  - Để ước lượng độ phức tạp của thuật toán ta dùng khái niệm bậc O lớn.

1.3. Thuật toán …

- *Định nghĩa 1:* Giả sử f[n] và g[n] là hai hàm xác định trên tập hợp các số nguyên dương. Ta nói f[n] có bậc O-lớn của g[n] và viết, f[n] = O(g[n]) nếu tồn tại một số C>0; sao cho với n đủ lớn. Các hàm f[n] và g[n] đều dương thì f[n] < C(g[n]).
  - VD: $f[n] = 3n^3 + 5n^2 + 2n + 8$ (n>0)

    $\Rightarrow$ Ta nói: $f[n] = O(n^3)$

1.3. Thuật toán …

- Một số tính chất:

1. Giả sử $f[n]$ là đa thức: $f[n] = a_d n^d + a_{d-1} n^{d-1} + \ldots + a_1 n + a_0$ trong đó $a_d > 0$. Khi đó: $f[n] = O(n^d)$.
2. Nếu $f_1[n] = O(g[n])$, $f_2[n] = O(g[n])$ thì $f_1 + f_2 = O(g)$.
3. Nếu $f_1 = O(g_1)$, $f_2 = O(g_2)$ thì $f_1 f_2 = O(g_1 g_2)$.
4. Nếu tồn tại giới hạn hữu hạn:

$$\lim_{n \to \infty} \frac{f[n]}{g[n]} \quad \text{thì } f = O(g)$$

5. Với mọi số $\varepsilon > 0$, $\log n = O(n^\varepsilon)$

1.3. Thuật toán …

- *Định nghĩa 2:* Một thuật toán được gọi là có độ phức tạp đa thức hoặc có thời gian đa thức, nếu số các phép tính cần thiết để thực hiện thuật toán không vượt quá $O(\log^d n)$, trong đó n là độ lớn của đầu vào và d là số nguyên dương nào đó.
- Nói cách khác nếu đầu vào là các số k bít thì thời gian thực hiện thuật toán là $O(k^d)$, tức là tương đương với một đa thức của k.

$\Rightarrow$ Khi giải một bài toán không những ta chỉ cố gắng tìm ra một thuật toán nào đó, mà còn muốn tìm ra thuật toán "tốt nhất". Đánh giá độ phức tạp là một trong những cách để phân tích, so sánh và tìm ra thuật toán tối ưu.

1.3. Thuật toán …

- Để hình dung "độ phức tạp" của các thuật toán khi làm việc với các số lớn, ta xem bảng dưới đây cho khoảng thời gian cần thiết để phân tích một số nguyên n ra thừa số nguyên tố bằng thuật toán nhanh nhất được biết hiện nay:

Số chữ số thập phân	Số phép tính bít	Thời gian
50	$1,4.10^{10}$	3,9 giờ
75	9.10^{12}	104 ngày
100	$2,3.10^{15}$	74 năm
200	$1,2.10^{23}$	$3,8.10^{9}$ năm
300	$1,5.10^{29}$	$4,9.10^{15}$ năm
500	$1,3.10^{39}$	$4,2.10^{25}$ năm

1.4. Độ mật hoàn thiện

- 1.4.1 Quan điểm về độ an toàn của hệ mật
- 1.4.2 Nhắc lại một số lí thuyết cơ bản về xác suất
- 1.4.3 Độ mật hoàn thiện

1.4.1 Quan điểm về độ an toàn của hệ mật

- Có hai quan điểm : Độ an toàn tính toán và độ an toàn không điều kiện
  - Độ an toàn tính toán
    - Liên quan đến nỗ lực tính toán để phá một hệ mật
    - Hệ mật an toàn về tính toán: thuật toán phá tốt nhất cần ít nhất N phép toán, N rất lớn, thực tế không có hệ mật nào thỏa mãn
    - Trên thực tế nếu có một phương pháp tốt nhất phá được hệ mật này nhưng yêu cầu thời gian lớn đến mức không chấp nhận được
    - Có thể quy về bài toán khó

- Độ an toàn không điều kiện
  - Không có hạn chế nào về khối lượng tính toán mà người giải mã được phép thực hiện.
  - Hệ mật an toàn không điều kiện nếu nó không thể bị phá ngay cả khi không hạn chế khả năng tính toán

  $\Rightarrow$ Độ an toàn không điều kiện của một hệ mật không thể nghiên cứu theo độ phức tạp tính toán mà sẽ dùng lí thuyết xác suất

1.4.2 Một số kiến thức cơ bản về lí thuyết xác suất

- *Định nghĩa 1:* X và Y là các biến ngẫu nhiên (bnn)
  - p(x): xác suất (xs) để X nhận giá trị x
  - p(y): xs để Y nhận giá trị y
  - p(x, y): xs đồng thời để X nhận giá trị x và Y nhận giá trị y.
  - p(x| y): xs để X nhận giá trị x với điều kiện (đk) Y nhận giá trị y.

- X và Y được gọi là độc lập nếu

$$p(x, y) = p(x).p(y), \text{ với } | x \in X \text{ và } | y \in Y.$$

- Quan hệ giữa xs đồng thời và xs có điều kiện được biểu thị theo công thức sau:

$$p(x,y) = p(x).p(y|x) = p(y).p(x|y)$$

- ĐL1: (ĐL Bayes)
  - Nếu p(y) > 0 thì:

$$p(x \mid y) = \frac{p(x).p(y \mid x)}{p(y)}$$

- *Hệ quả 1*
  - X và Y là các biến độc lập khi và chỉ khi:

$$p(x|y) = p(x) \text{ với mọi } x, y.$$

- Giả sử:
  - Mỗi khóa cụ thể chỉ dùng cho một bản mã
  - Trên không gian bản rõ có một phân bố xs
  - $p_P(x)$: xs tiên nghiệm để bản rõ xuất hiện
  - Khóa K được chọn theo một xs $p_K(K)$
  - K và x độc lập

- Với mỗi khóa K, thì tập các bản mã có thể:

$$C(K) = \{e_K(x) : x \in P\}$$

- Hai phân bố xs trên P và K sẽ tạo nên phân bố xs trên C

$$p_C(y) = \sum_{\{K:y \in C(K)\}} p_K(K) p_P(d_K(y))$$

- Xs có đk:

$$p_C(y \mid x) = \sum_{\{K:x = d_K(y)\}} p_K(K)$$

- Và tính được:

$$p_P(x \mid y) = \frac{p_P(x) \sum_{\{K:x = d_K(y)\}} p_K(K)}{\sum_{\{K:y \in c(K)\}} p_K(K) p_P(d_K(y))}$$

- Ví dụ 1.
  - Giả sử P ={a, b} với $p_P(a) = 1/4$, $p_P(b) = 3/4$.
  - Cho K = {K1, K2, K3} với $p_K(K1) = 1/2$, $p_K(K2) = p_K(K3) = 1/4$.
  - Giả sử C = {1, 2, 3, 4}
  - $e_{K1}(a) = 1$, $e_{K2}(a) = 2$, $e_{K3}(a) = 3$, $e_{K1}(b) = 2$, $e_{K2}(b) = 3$, $e_{K3}(b) = 4$

$\Rightarrow$ Tính các xs của các bản mã trên C và các xs có đk của bản rõ khi biết các bản mã.

- Áp dụng các công thức ta tính được
-
$$p_C(1) = \sum_{\{K:y \in C(K)\}} p_K(K)\, p_P(d_K(y)) = p_K(K_1) \cdot p_P(d_{K_1}(1)) = p_K(K_1) \cdot p_P(a) = \frac{1}{2} \cdot \frac{1}{4} = \frac{1}{8}$$

Tương tự có: $p_C(2) = 7/16$, $p_C(3) = 1/4$,

$p_C(4) = 3/16$

-
$$p_P(a \mid 1) = \frac{p_P(a) \cdot \sum_{\{K:a=d_K(1)\}} p_K(K)}{p_C(1)} = \frac{p_P(a) \cdot p_K(K_1)}{p_C(1)} = \frac{\frac{1}{4} \cdot \frac{1}{2}}{1/8} = 1$$

- Tương tự có: $p_P(a|1) = 1$, $p_P(a|2) = 1/7$, $p_P(b|1) = 0$, …

1.4.3 Độ mật hoàn thiện

- ĐN 2: Một hệ mật có độ mật hoàn thiện nếu:

  $p_P(x|y) = p_P(x)$, với mọi x thuộc P, y thuộc C

- ĐL 2: Giả sử 26 khóa trong mã dịch vòng (MDV) có xs như nhau và bằng 1/26. Khi đó MDV sẽ có độ mật hoàn thiện với mọi phân bố xs của bản rõ

- Giả sử $p_C(y)>0$, mọi y ϵ C ($p_C(y)= 0$ thì loại ra khỏi C). Đk $p_P(x|y) = p_P(x)$, với mọi x ϵ P, y ϵ C tương đương với $p_C(y) = p_C(y|x)$. Khi đó cố định x ϵ P, mỗi y ϵ C :$p_C(y) = p_C(y|x)>0$, tức là có ít nhất một khóa K để $e_K(x) = y$ → $|C| \leq |K|$.

  Mà $|P| \leq |C|$ nên $|P| \leq |C| \leq =|K|$

- ĐL 3

  Giả sử (P, C, K, E, D) là một hệ mật, trong đó

  |K| = |C| = |P|. Khi đó hệ mật hoàn thiện khi và chỉ khi mỗi khóa K được dùng với xs như nhau bằng 1/|K|, và mỗi

  x ϵ P , mỗi y ϵ C có một khóa duy nhất K sao cho $e_K(x) = y$.

- Ví dụ hệ mật của Vernam (OTP)
  - Giả sử n 1 là một số nguyên và P = C = K = $(Z_2)^n$. Với K ϵ $(Z_2)^n$, ta xác định $e_K(x)$ là tổng vec tơ theo modulo 2 của K và x (tương đương với phép hoặc loại trừ của hai dãy bit). Như vậy, nếu x = (x1,x2,…,xn) và K= (K1,K2,…,Kn) thì:

    $e_K(x)$ = (x1+K1,x2+K2,…,xn+Kn) mod 2
  - Phép mã hóa là đồng nhất với phép giải mã, tức là nếu

    y = (y1, y2, …, yn) thì:

    $d_K(y)$ = (y1 + K1, y2 + K2, …, yn + Kn) mod 2.

- Ví dụ: $x = (x_1, x_2, x_3) = (101, 010, 111)$;

  $K = (K_1, K_2, K_3) = (010, 100, 110)$

Khi đó phép mã hoá:

$y = e_K(x) = (101 \oplus 010, 010 \oplus 100, 111 \oplus 110) = (111, 110, 001)$

và phép giải mã:

$x = d_K(y) = (111 \oplus 010, 110 \oplus 100, 001 \oplus 110) = (101, 010, 111)$

1.5 Entropy

- 1.5.1 Entropy
- 1.5.2 Một số tính chất về entropy

1.5.1 Entropy

- Entropy là khái niệm trong lí thuyết thông tin do Shannon đưa ra vào năm 1948.
- Có thể coi entropy là đại lượng đo thông tin hay còn gọi là độ bất định, nó được tính như một hàm phân bố xs, kí hiệu là H(X).
- Ví dụ tính entropy của phép tung đồng xu
- Nhận xét:
  - Một biến cố xảy ra với xs 2^{-n} có thể mã hóa được bằng một xâu bit có độ dài n

- Tổng quát có thể coi một biến cố xảy ra với xs p thì có thể mã hóa bằng một xâu bit có độ dài xấp xỉ $-\log_2 p$.
- Nếu cho trước $p_1, p_2, \ldots, p_n$ của bnn X, khi đó độ đo thông tin là trọng số trung bình của các lượng $-\log_2 p_i$

ĐN 3:

- Giả sử X là một biến ngẫu nhiên lấy các giá trị trên một tập hữu hạn theo phân bố xs p(X). Khi đó entropy của phân bố xs này được định nghĩa là lượng:

$$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i$$

- Nếu các giá trị có thể của X là x_i, $1 \leq i \leq n$ thì ta có:

$$H(X) = -\sum p(X = x_i) \log_2 p(X = x_i)$$

- Nhận xét:
  - $\log_2 p_i$ không xác định nếu $p_i = 0$, nên đôi khi entropy được định nghĩa là tổng tương ứng trên tất cả các xs khác 0. Vì $\lim_{x \to 0} x \log_2 x = 0$ nên thực tế cũng không có trở ngại gì nếu cho $p_i = 0$, với i nào đó. Tuy nhiên ta sẽ tuân theo giả định là khi tính entropy của một phân bố xs p_i, thì H(X) được tính trên các chỉ số i sao cho p_i khác 0.
  - Cơ số của logarit được chọn tùy ý, giá trị entropy chỉ thay đổi một hằng số.
  - Nếu $p_i = 1/n$ với $1 \le i \le n$ thì $H(X) = \log_2 n$.
  - $H(X) \ge 0$. $H(X) = 0$ khi và chỉ khi $p_i = 1$ với i nào đó và $p_j = 0$ với mọi $j \ne i$.
  - Ta cũng có thể tính H(P), H(C), H(K) của hệ mật.

1.5.2 Các tính chất của entropy

- Trước tiên nhắc lại một số kiến thức
  - f lồi trên khoảng I: $f(\frac{x+y}{2}) \geq \frac{f(x)+f(y)}{2}$, với mọi x, y $\in$ I
  - f lồi thực sự trên I nếu: $f(\frac{x+y}{2}) > \frac{f(x)+f(y)}{2}$, với mọi x, y $\in$ I, x $\neq$ y.
  - ĐL 5 (Bất đẳng thức Jensen)

Giả sử f là một hàm lồi thực sự và liên tục trên khoảng I, $\sum_{i-1}^{n} a_i = 1$ và với, $1 \leq i \leq n$. Khi đó: $\sum_{i-1}^{n} a_i f(x_i) \leq f\left(\sum_{i-1}^{n} a_i x_i\right)$ trong đó $x_i \in I$, $1 \leq i \leq n$. Ngoài ra dấu "=" xảy ra khi và chỉ khi $x_1 = \ldots = x_n$.

- Các tính chất:
  - ĐL 5:Giả sử X là một biến ngẫu nhiên có phân bố xs $p_1, p_2, \ldots, p_n$, trong đó $p_i > 0$, $1 \leq i \leq n$. Khi đó $H(X) \leq \log_2 n$. Dấu "=" xảy ra khi và chỉ khi $p_i = 1/n$, $1 \leq i \leq n$
  - ĐL 6: $H(X, Y) \leq H(X) + H(Y)$

    Đẳng thức xảy ra khi và chỉ khi X và Y là các biến cố độc lập.

- ĐN 5:

  X và Y là hai bnn, khi đó với giá trị xác định bất kì y của Y, ta có một phân bố xs có đk p(X|y). Rõ ràng là:

$$H(X \mid y) = -\sum_{x} p(x \mid y) \log_2 p(x \mid y)$$

- Ta định nghĩa entropy có điêu kiện H(X| Y) là trung bình trọng số ứng với các xs p(y) của entropy H(X| y) trên mọi giá trị có thể y.
- H(X| Y) được tính bằng:

$$H(X \mid Y) = -\sum_{y} \sum_{x} p(y) p(x \mid y) \log_2 p(x \mid y)$$

- ĐL 7: H(X,Y) = H(X|Y) +H(Y)
- HQ 1: H(X|Y) ≤ H(X), dấu "=" xảy ra khi và chỉ khi X, Y độc lập

1.6 Các khóa giả và khoảng duy nhất

- Trong phần này ta sẽ áp dụng các kết quả về entropy ở trên cho các hệ mật
- Trước hết ta sẽ chỉ ra quan hệ giữa các entropy của các thành phần trong hệ mật.
  - ĐL 8: Giả sử (P, C, K, E, D) là một hệ mật, khi đó:

$$H(K|C) = H(K) + H(P) - H(C)$$

1.6 Các khóa giả …

- Khóa giả: Các khóa mà thám mã có thể rút ra nhưng không phải là khóa đúng
  - Ví dụ: giả sử thám mã thu được bản mã WNAJW được mã bằng phương pháp MDV. Chỉ có 2 xâu bản rõ có ý nghĩa là river và arena tương ứng với các khóa F (=5) và W (=22). Trong hai khóa này có 1 khóa đúng và khóa còn lại khóa giả.

$\Rightarrow$ Mục đích là tìm ra giới hạn cho số trung bình các khóa giả

- Kí hiệu lượng thông tin trung bình trên một kí tự trong một xâu có nghĩa của bản rõ là H_L
- Dùng entropy, ta có thể lấy H(P) làm xấp xỉ bậc nhất cho H_L
- Tuy nhiên các kí tự liên tiếp trong một ngôn ngữ không độc lập với nhau nên sẽ làm giảm entropy. Ta sẽ tính entropy của phân bố xs của các bộ đôi rồi chia cho 2 để làm xấp xỉ bậc 2 cho H_L. Cứ như vậy trong trường hợp tổng quát, ta định nghĩa P^n là bnn có phân bố xs là phân bố xs của tất cả các bộ n của bản rõ và dùng định nghĩa sau

- ĐN 8: Giả sử L là một ngôn ngữ tự nhiên, entropy của L được xác định là lượng sau: $H_L = \lim_{n \to \infty} \frac{H(P^n)}{n}$

Độ dư của L là: $R_L = 1 - (H_L / \log_2 |\wp|$

- Nhận xét:
  - H_L đo entropy trên mỗi kí tự của ngôn ngữ L
  - R_L đo phần "kí tự vượt trội" là phần dư vì entropy của một ngôn ngữ ngẫu nhiên là $\log_2|P|$.
- Dựa vào giá trị của H_L ta có thể đánh giá được lượng thông tin trung bình của một ngôn ngữ, ví dụ với L là Anh ngữ thì $1.0 \leq H_L \leq 1.5$. Giả sử lấy $H_L = 1.25$ thì độ dư là 75% tức là dùng thuật toán Huffman (phép mã hóa nén) có thể tìm ra được một đơn ánh cho các bộ n (n đủ lớn) mà nén văn bản tiếng Anh xuống còn 1/4 văn bản gốc

- Với các phân bố xs đã cho trên K và P^n, có thể xác định được phân bố xs trên C^n là tập các bộ n của bản mã. Với y ϵ C^n, định nghĩa:

$$K(y) = \{K \in K : \exists x \in P^n, p_{P^n}(x) > 0, e_K(x) = y\}$$

- Như vậy nếu y là dãy quan sát được của bản mã thì số khoá giả là |K(y)|-1
- Kí hiệu $\overline{s}_n$ là số trung bình các khoá giả (trên tất cả các xâu bản mã có thể độ dài n) thì:

$$\overline{s}_n = \sum_{y \in C^n} p(y)(|K(y)| - 1) = \sum_{y \in C^n} p(y)|K(y)| - \sum_{y \in C^n} p(y)$$

$$\overline{s}_n = \sum_{y \in C^n} p(y)|K(y)| - 1$$

- Với n đủ lớn ta có ước lượng

$$\log_2(\overline{s}_n + 1) \geq H(K) - nR_L \log_2 |P|$$

- Nếu các khoá được chọn với xs như nhau (khi đó H(K) có giá trị lớn nhất) ta có định lí sau:
- ĐL 9: Giả sử (P, C, K, E, D) là một hệ mật trong đó |C| = |P| và các khóa được chọn đồng xác suất. Giả sử R_L là độ dư của ngôn ngữ gốc, khi đó với một xâu bản mã độ dài n cho trước (n là số đủ lớn), số trung bình các khóa giả thỏa mãn bất đẳng thức sau:

$$\bar{s}_n \geq \{|K|/(|P|^{nR_L})\} - 1$$

- Lượng $|K|/(|P|^{nR_L}) - 1$ tiến tới 0 theo hàm mũ khi n tăng, n nhỏ ước lượng này có thể không chính xác vì $H(P^n)/n$ không phải là ước lượng tốt cho H_L nếu n nhỏ.

- ĐN 9: Khoảng duy nhất của một hệ mật được định nghĩa là giá trị của n mà ứng với giá trị này, số khóa giả trung bình bằng 0 (kí hiệu giá trị này là n_0). Điều đó có nghĩa n_0 là độ dài trung bình cần thiết của bản mã để thám mã có thể tính toán một cách duy nhất với thời gian đủ lớn.