Một số hệ mật mã đơn giản

Bởi:
Khoa CNTT ĐHSP KT Hưng Yên

Mã dịch chuyển (shift cipher)

Đặt $P=C=K=Z_{26}$. Với $0 \le K \le 25$, định nghĩa:

$e_K(x) = x + K \bmod 26$

và

$d_K(y) = y - K \bmod 26$

(x, y Z_{26}).

Trường hợp đặc biệt K=3 ứng với hệ mật mã Caesar.

Ví dụ:

Plain: meet me after the toga party

Cipher: PHHW PH DIWHU WKH WRJD SDUWB

Mã thay thế (substitution cipher)

Đặt $P=C=Z_{26}$. Với K gồm tất cả các hoán vị có thể của 26 ký hiệu 0, 1, …, 25. Với mỗi K K định nghĩa:

$e_K(x) = K(x) \bmod 26$

và

$d_K(y) = K^{-1}(y) \bmod 26$

Trong đó K^{-1} là hoán vị ngược của K.

Ví dụ:

Khóa K:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
X	N	Y	A	H	P	O	G	Z	Q	W	B	T	S	F	L	R	C	V	M	U	E	K	J	D	I

Khóa K^{-1}

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
d	l	r	y	v	o	h	e	z	x	w	p	t	b	g	f	j	q	n	m	u	s	k	a	c	i

Cipher: MGZVYZLGHCMHJMXSSFMNHAHYCDLMHA

Hệ mật mã Affine

Đặt $P=C= Z_{26}$ và đặt

K={(a, b) Z_{26}X Z_{26}: gcd(a, 26)=1}.

Với K=(a, b) K, định nghĩa:

$e_K(x) = ax+b$ mod 26

và

$d_K(y) = a^{-1}(y - b)$ mod 26

(x, y Z_{26}).

Trong đó $a^{-1} Z_{26}$, sao cho $aa^{-1} \equiv a^{-1}a \equiv 1(\text{mod}26)$.

Ví dụ:

K=(7, 3)

Giải thuật Euclid mở rộng:

Tính phần tử nghịch đảo: a^{-1}

1. $n_0 = n$

2. $a_0 = a$

3. $t_0 = 0$

4. t = 1

5. q = $\left\lfloor \frac{n_0}{a_0} \right\rfloor$

6. r = n_0 – q x a_0

7. while r > 0 do

8. temp = t_0 – q x t

9. If temp 0 then temp = temp mod n

10. If temp < 0 then temp = n – ((-temp) mod n)

11. t_0 = t

12. t = temp

13. n_0 = a_0

14. a_0 = r

15. q = $\left\lfloor \frac{n_0}{a_0} \right\rfloor$

16. r = n_0 – q x a_0

17. if a_0 1 then

a không có nghịch đảo

else

a^{-1} = t mod n

Hệ mật mã Vigenere

Đặt m là một số nguyên dương. Định nghĩa $P=C=K= (Z_{26})^m$. Với một khóa K=($k_1,k_2,...,k_m$), chúng ta định nghĩa:

$e_K(x_1,x_2,...,x_m) = (x_1 + k_1,x_2 + k_2,...,x_m + k_m)$

và

$d_K(y_1,y_2,...,y_m) = (y_1 - k_1, y_2 - k_2, ..., y_m - k_m)$

Trong đó các phép +, - được thực hiện trên trường Z_{26}.

Hệ mật mã Hill

Đặt m là một số nguyên dương. Đặt $P=C=(Z_{26})^m$ và đặt

K={m x m là ma trận khả nghịch trên Z_{26}}.

Với K K, định nghĩa:

$e_K(x) = xK \bmod 26$

và

$d_K(y) = yK^{-1} \bmod 26$

(x, y Z_{26}).

Trong đó: $KK^{-1} = I_m$ với I_m là ma trận đơn vị.

Ví dụ: Với m=2; K= $\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$, $K^{-1}= \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$

có x=(9, 20), xK=(3, 4); có x=(11, 24), xK=(11, 22);

Mã hoán vị (permutation cipher)

Đặt m là một số nguyên dương. Đặt $P=C=(Z_{26})^m$ và đặt K là tập tất cả các hoán vị của tập {1, …, m}. Với K K, định nghĩa:

$e_K(x_1,...,x_m) = (x_{K(1)},...,x_{K(m)}) \bmod 26$

và

$d_K(y_1,...,y_m) = (y_{K^{-1}(1)},...,y_{K^{-1}(m)}) \bmod 26$

Trong đó K^{-1} là hoán vị ngược của K.

Mã dòng (stream cipher)

Định nghĩa

Một hệ mã dòng là một bộ 7 (*P, C, K, L, F,ε,D*), thỏa mãn các điều kiện sau đây:

1. *P* là tập hữu hạn các bản tin rõ
2. *C* là một tập hữu hạn các bản tin đã mã hóa
3. *K* là không gian khóa, là tập hữu hạn các khóa
4. *L* là tập các dòng khóa
5. *F =(f 1 , f 2, ...) là bộ sinh. Với i>=1: f i : KxP i-1 -> L*
6. Với mỗi z <*L,* tồn tại một giải thuật mã hóa $e_z \in$ εvà một giải thuật giải mã $d_z \in$ *D. Trong đó:* $\boldsymbol{e_z}$**:***P* → *C* và d_z:*C* → *P* là các hàm sao cho $d_z(e_z(x)) = x$ với mọi x *P.*