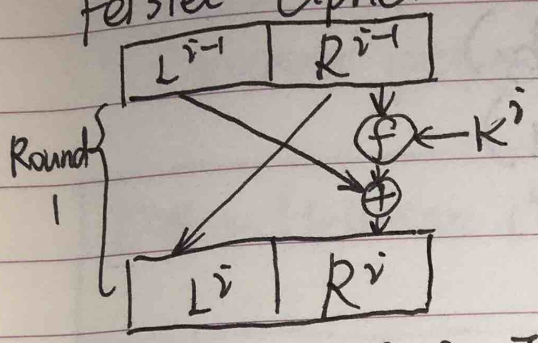
DES (Data Encryption standard):

K: large key
↓ key schedule
subkeys

Feistel Cipher:



K^i is a subkey, f is a function not necessarily one-to-one.

start $L^0R^0 = IP(x)$, IP Permutation. (x: plaintext)

Then n rounds of Feistel Cipher.

STOP $y = IP^{-1}(R^{n+1}L^{n+1})$ (y: ciphertext)

Permutations:

Example: $IP = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 3 & 1 & 6 \end{pmatrix}$

$x_i \longrightarrow x_{IP(i)}$ $\quad x_1 \longrightarrow x_{IP(1)} = x_4$

$x_2 \longrightarrow x_{IP(2)} = x_5$

We only need the second now.

4	5	2	3	1	6

All are the some permutations

4	5	2
3	1	6

4	5
2	3
1	6

Chapter 5: Public-key cryptography

Alice —— Oscar —— Bob

$y = e_k(x)$ ——→ y = online (Oscar) ——→ $x = d_k(y)$ } symmetric-key ~~cryptography~~ cryptosystems

x = plaintext y = ciphertext

Diffie-Hellman 1976. RSA — 1977. (Rivest, Shamir, Adleman.)

Diffie-Hellman key Exchange:

Step 1: p, g, are public numbers
- p: prime
- g: primitive root modulu p → $g^p = 1 \bmod p$.

~~[crossed out]~~

Step 2: Alice choose a secret integer a such that $1 < a < p$.

Step 3: Bob changes a secret integer b, $1 < b < p$.

Step 4: Alice sends $g^a \bmod p$ to Bob.

Step 5: Bob sends $g^b \bmod p$ to Alice.

Step 6: Alice completes $(g^b)^a \bmod p$.

Step 7: Bob completes $(g^a)^b \bmod p$.

→ $(g^b)^a = (g^a)^b$ ← shared key.

Example 1. ① $p = 23$, $g = 5$ — Oscar know, p=23, g=5 & 19 & 8 &

② Alice chooses $a = 6$

③ Bob chooses $b = 15$

④ Alice sends $g^a \bmod p$, $5^6 \bmod 23 = 15625 \bmod 23 = 8$

⑤ Bob sends $g^b \bmod p$, $5^{15} \bmod 23 = 19$

⑥ Alice computes $(g^b)^a \bmod p$, $(5^{15})^6 \bmod 23 = (19)^6 \bmod 23 = 2$

⑦ Bob: $(5^6)^{15} \bmod 23 = (8)^{15} \bmod 23 = 2$

Shannon's information Theory:
- Elementary probability — Perfect Secrecy.
- Entropy (How to measure information)

Recall that a cryptosystem is a five-tuple
(P, C, K, e, d) ← decryption function.
↑ plaintext ↑ cipher-text ↑ keys ↑ encryption function

P. C. K are finite sets.
e is a one-to-one function.

Definitions: $C(K) = e_K(P)$ = image of P under e_K.
$K(y) = \{K \in K : y \in C(K)\}$
$K(x, y) = \{K \in K : e_K(x) = y\}$.

Example: $P = \{x_1, x_2, x_3\}$
$C = \{y_1, y_2, y_3, y_4, y_5\}$.
$K = \{k_1, k_2, k_3, k_4\}$.

Encryption Matrix: → cryptosystem

	x_1	x_2	x_3
k_1	y_1	y_2	y_5
k_2	y_4	y_3	y_2
k_3	y_2	y_4	y_5
k_4	y_5	y_1	y_3.

MAT348: Review.

① Shift cipher:

The encryption function e_k: $e_k(x) = (x+k) \bmod 26$.

The decryption function d_k: $d_k(y) = (y-k) \bmod 26$.

$a \equiv b \bmod m \Rightarrow a - b = km$ $\quad$ $a \bmod m = r \Rightarrow a = tm + r$.

E.g. $4 \equiv 30 \bmod 26 \Rightarrow 4 - 30 = -26 = -1 \times 26$.

$-30 \bmod 26 = 22 \Rightarrow -30 + 26 \times 2 = 22$

② Substitution Cipher:

The encryption function: e_π: $e_\pi(x) = \pi(x)$

The decryption function: d_π: $d_\pi(y) = \pi^{-1}(y)$

E.g. $\pi = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 1 & 0 & 2 \end{pmatrix}$ $\quad$ $\pi^{-1} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 1 & 3 & 0 \end{pmatrix}$

The number of permutation of n letter is $n!$

E.g. ~ of 4 letter is $4! = 24$.

③ Affine Cipher:

The encryption function e_k: $e_k(x) = (ax+b) \bmod 26$.

$d_k(y) = a^{-1}(y-b) \bmod 26$. $\quad$ $K = \{(a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}, \gcd(a,26) = 1\}$.

The number of keys in the Affine cipher over $\mathbb{Z}_n$ is $\phi(n) \cdot n$

E.g. in $\mathbb{Z}_{26}$, $\phi(26) \cdot 26 = \phi(2) \cdot \phi(13) \cdot 26 = (2-1)(13-1) \times 26 = 312$.

E.g. $K = (5, 8)$, $e_K(x) = (5x+8) \bmod 26$.

$K = (7, 4) \Rightarrow d_K(y) = 7^{-1}(y-4) \bmod 26 = 15(y-4) \bmod 26$.

In $\mathbb{Z}_5$, the multiplicative inverse of 3 is 2 $\Rightarrow (3 \cdot 2) \bmod 5 = 1 \Leftrightarrow 3^{-1} \bmod 5 = 2$.

If $\gcd(a,n) = 1$, a is invertible in $\mathbb{Z}_n$.

☆ We can use Euclidean algorithm to Find $\gcd(2196, 6972) = 12$

i	x	y	r
0	2196	6972	$6972 \div 2196 = 3 \ldots 384$
1	384	2196	276
2	276	384	108
3	108	276	60
4	60	108	48
5	48	60	12
6	12	48	0
7	0		

RSA 2: Solve the following system of congruences.

$x \equiv 4 \bmod 7,\ x \equiv 3 \bmod 11,\ x \equiv 8 \bmod 13. \Rightarrow x = ???$

$\because a_1=4,\ a_2=3,\ a_3=8;\ m_1=7,\ m_2=11,\ m_3=13.$

$m_1=7,\ m_2=11,\ m_3=13$ } $\gcd(7,11)=1,\ \gcd(7,13)=1,\ \gcd(11,13)=1 \Rightarrow M=m_1\times m_2\times m_3=1001$

$M_1=1001/7=143,\ M_2=1001/11=91,\ M_3=77.$

$y_1=143^{-1} \bmod 7=(143 \bmod 7)^{-1} \bmod 7=3^{-1} \bmod 7=5.$

$y_2=91^{-1} \bmod 11=4 \qquad y_3=77^{-1} \bmod 13=12$

$x=[a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3] \bmod 1001 = 333.$

(11) ElGamal Cryptosystem:

$e_k(x)=(\alpha^r \bmod p,\ x\beta^r \bmod p)$

$d_k(y_1,y_2)=y_2(y_1^a)^{-1} \bmod p.$

Eg. Suppose Bob chooses $p=2579,\ \alpha=2,\ \beta=949$, Alice wants to send $x=1299$, $r=853.$

$\therefore e_k(x)=(2^{853} \bmod 2579,\ 1299\times 949^{853} \bmod 2579)=(435, 2396).$

When Bob receives $(435, 2396)$, he can use $a=\log_\alpha \beta=\log_2 949=765.$

$d_k(435, 2396)=2396\times(435^{765})^{-1} \bmod 2579=1299.$

Eg. $\log_9 11=2 \Rightarrow 9^2=11 \bmod 14.$

How to Find $\log_7 2$ in $\mathbb{Z}_{23}$.

$\because |\mathbb{Z}_{\Phi(n)}| = |\mathbb{Z}_{\Phi(23)}| = |\mathbb{Z}_{22}| = 5.$

1. $7^0=1,\ 7^5=17,\ 7^{10}=13,\ 7^{15} \bmod 23=14,\ 7^{20}=8.$
2. $2(7^{-1})^y=2\cdot 10^y \Rightarrow 2\cdot 10^0=2,\ 2\cdot 10^1=20,\ 2\times 10^2=16,\ 2\times 10^3=22,\ 2\times 10^4=13.$

Then $\log_7 2=(5\times 2+4) \bmod 23=14$

(13) Involutory keys over $\mathbb{Z}_{26}$ in Affine Cipher

$x+\alpha = x-\alpha \bmod 26 \Leftrightarrow 2\alpha = 0 \bmod 26$.

$\alpha = 0$ or $\alpha = 13 \bmod 26$.