DES

message: 0101111 0

key: 0101101010

key generation

P10: 3 5 2 7 4 10 1 9 8 6

0111100100

0111 1 00100

LS1: 11110 01000

P8: 6 3 7 4 8 5 10 9

01110000 → K1

LS2: 11011 00001

P8: 00010110 → K2

Encryption

IP: 2 6 3 1 4 8 5 7

1 1 0 0 1 0 1 1

1 1 0 0 1 0 1 1

E/P: 1 0 1 1

4 1 2 3 2 3 4 1

1 1 0 1 0 1 1 1

Xor: $\oplus$ 0 1 1 1 0 0 0 0 $\rightarrow K_1$

1 0 1 0 0 1 1 1

S0: 1 0 1 0 $\rightarrow$ 1 0

S1: 0 1 1 1 $\rightarrow$ 1 1

1 0 1 1

P4: 2 3 4 1

0 1 1 1

$\oplus$ 1 1 0 0

1 0 1 1

Round 2.

swap: 1011 1011

E/P : 1011

4 1 2 3 2 3 4 1

1 1 0 1 0 1 1 1

Xor : ⊕ 0 0 0 1 0 1 1 0 → K2

1 1 0 0 0 0 0 1

S0 : 1100 → 01

S1 : 0001 → 10

0110

P4 : 2 3 4 1

1 1 0 0

XOR(L-S) : 1011

0111

IP-1 : 0111 1011

4 1 3 5 7 2 8 6

---

1 0 1 1 1 1 1 0

example 2 : DES

key : 1010000010

P10 : 3 5 2 7 4 1 0 1 9 8 6

1 0 0 0 0 1 1 1 0 0

1 0 0 0 0 0 1 1 0 0

LS1 : 0 0 0 0 1 1 1 0 0 0

P8 : 6 3 7 4 8 5 1 0 9

1 0 1 0 0 1 0 0 → key1

LS2 : 0 0 1 0 0 0 0 0 1 1

P8 : 6 3 7 4 8 5 1 0 9

0 1 0 0 0 0 1 1 → key2

encryption

$S_0 \leftarrow$ 1001 0111 $\rightarrow$ R.S

IP: 2 6 3 1 4 8 5 7

0 1 0 1 1 1 0 1

$L_S \leftarrow$ 0101 1101 $\Rightarrow$ R.S

EP : 1101

4 1 2 3 2 3 4 1

1 1 1 0 1 0 1 1

XOR $\oplus$ 1 0 1 0 0 1 0 0 $\rightarrow$ key 1

0 1 0 0 1 1 1 1

$S_0 \rightarrow$ 0100 $\rightarrow$ 11

$S_1 \rightarrow$ 1111 $\rightarrow$ 11

P4 $\rightarrow$ 2 4 3 1

1 1 1 1

$

Xor 1111

⊕ 0101 → L.S.

$010

Round 2.

Swap: 1101 1010

E/P: 1010

41232341

01010101

Xor ⊕ 01000011 → key2

00010110

S0: 0001 → 11

S1: 0110 → 11

P4 : 1111

2431

1111

Xor $\oplus$ 1101 $\rightarrow$ L.S

0010

IP-1 : 00101010

41357286

00111000

AES

example 1

p : 1101 0111 0010 1000

key : 0100 1010 1111 0101

Key generation

W_0 = 0100 1010

W_1 = 1111 0101

$W_2 = W_0 \oplus RCon(1) \oplus (S\text{-}Box(Rot(W_1)))$

$= 0100\ 1010 \oplus 1000\ 0000 \oplus (S\text{-}Box(0101\ 1111))$

$= 0100\ 1010 \oplus 1000\ 0000 \oplus 0001\ 0111$

$= 0100\ 1010 \oplus 1001\ 0111$

W2 = 1101 1101

$W3 = W2 \oplus W1 = 1101\ 1101 \oplus 1111\ 0101$

$W_3 = 0010\ 1000$

$W4 = W2 \oplus Rcon(2) \oplus (S\text{-}box(Rot(W3)))$

$= 1101\ 1101 \oplus 0011\ 0000 \oplus (S\text{-}box(1000\ 0010))$

$= 1101\ 1101 \oplus 0011\ 0000 \oplus 0110\ 1010$

$= 1101\ 1101 \oplus 0101\ 1010$

$W4 = 1000\ 0111$

$W5 = W4 \oplus W3 = 1000\ 0111 \oplus 0010\ 1000$

$= 1010\ 1111$

$K_0 = 0100\ 1010\ 1111\ 1001$

$K1 = 1101\ 1101\ 0010\ 1000$

$K2 = 1000\ 0111\ 1010\ 1111$

Encryption :

add round key : $P \oplus K_0$

$1101\ 0111\ 0010\ 1000 \oplus 0100\ 1010\ 1111\ 0101$

$= 1001\ 1101\ 1101\ 1101$

Sub nib : $\overset{2}{0010}\ \overset{E}{1110}\ \overset{E}{1110}\ \overset{E}{1110}$

$$\begin{bmatrix} 2 & E \\ E & E \end{bmatrix}$$

Shiftrows $= \begin{bmatrix} 2 & E \\ E & E \end{bmatrix}$ (no change)

↳ exchange pos 2 and 4
(swap)

Mix columns : $\begin{bmatrix} 2 & E \\ E & E \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}$

$$= \begin{bmatrix} (2 * 1 \oplus E * 4) & (E * 1 \oplus E * 4) \\ (2 * 4 \oplus E * 1) & (E * 4 \oplus E * 1) \end{bmatrix}$$

$$\begin{bmatrix} 2 \oplus D & E \oplus D \\ 8 \oplus E & D \oplus E \end{bmatrix}$$

$$= \begin{bmatrix} 0010 \oplus 1101 & 1110 \oplus 1101 \\ 1000 \oplus 1110 & 1101 \oplus 1110 \end{bmatrix}$$

$$= \begin{bmatrix} 1111 & 0011 \\ 0110 & 0011 \end{bmatrix}$$

1111 0110 0011 0011

Add round key :

1111 0110 0011 0011 $\oplus$ K_1 (W2, W3)

= 1111 0110 0011 0011 $\oplus$ 1101 1101 0010 1000

= 0010 1011 0001 1011

Subnib (S-box) : A 3 4 3

$$\begin{bmatrix} A & 4 \\ 3 & 3 \end{bmatrix}$$

shift row $\begin{bmatrix} A & 4 \\ 3 & 3 \end{bmatrix}$ no change

add round key :

1010 0011 0100 0011 $\oplus$ K_2 (W_4, W_5)

= 1010 0011 0100 0011 $\oplus$ 1000 0111 1010 1111

= 0010 0100 1110 1100

example 2

Key generation:

$W_0 = 0110\ 1100$

$W_1 = 1011\ 0010$

$W_2 = W_0 \oplus Rcon(1) \oplus (S\text{-}box(Rot(W_1)))$

$= 0110\ 1100 \oplus 1000\ 0000 \oplus S\text{-}box(0010\ 1011)$

$= 0110\ 1100 \oplus 1000\ 0000 \oplus 1010\ 0011$

$= 0110\ 1100 \oplus 0010\ 0011$

$= 0100\ 1111$

$W_3 = W_2 \oplus W_1 = 0100\ 1111 \oplus 1011\ 0010$

$= 1111\ 1101$

$W_4 = W_2 \oplus Rcon(2) \oplus (S\text{-}box(Rot(W_3)))$

$= 0100\ 1111 \oplus 0011\ 0000 \oplus S\text{-}box(1110\ 1111)$

$= 0100\ 1111 \oplus 0011\ 0000 \oplus 1110\ 0111$

$= 0100\ 1111 \oplus 1101\ 0111 = 1001\ 1000$

$W_5 = W_4 \oplus W_3 = 1001\ 1000 \oplus 1111\ 1101$

$= 0110\ 0101$

$K_0 = 0110\ 1100\ 1011\ 0010$

$K_1 = 0100\ 1111\ 1111\ 1101$

$K_2 = 1001\ 1000\ 0110\ 0101$

Encryption:

add round key: $P \oplus K_0$

$1010\ 1101\ 0110\ 0011 \oplus 0110\ 1100\ 1011\ 0011$

$= 1100\ 0001\ 1101\ 0001$

Sub nib: C 4 E 4

$$\begin{bmatrix} C & E \\ 4 & 4 \end{bmatrix}$$

Shift row: $\begin{bmatrix} C & E \\ 4 & 4 \end{bmatrix}$ no change

mix column: $\begin{bmatrix} C & E \\ 4 & 4 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}$

$= \begin{bmatrix} C * 1 \oplus E * 4 & 4 * 1 \oplus 4 * 4 \\ C * 4 \oplus E * 1 & 4 * 4 \oplus 4 * 1 \end{bmatrix}$

$= \begin{bmatrix} C \oplus D & 4 \oplus 3 \\ 5 \oplus E & 3 \oplus 4 \end{bmatrix}$

$$\begin{bmatrix} 1100 \oplus 1101 & 0100 \oplus 0011 \\ 0101 \oplus 1110 & 0011 \oplus 0100 \end{bmatrix}$$

$$= \begin{bmatrix} 0001 & 0111 \\ 1011 & 0111 \end{bmatrix}$$

~~add~~ 0001 1011 0111 0111

$\rightarrow K1$

add round key:

0001 1011 0111 0111 $\oplus$ K1 (W2, W3)

= 0001 1011 0111 0111 $\oplus$ 0100 1111 1111 1101

= 0101 0100 1000 1010

subnib:

0001 1101 0110 0000

Shift rows:

0001 0000 0110 1101

addroundkey $\rightarrow K_2$:

0001 0000 0110 1101 $\oplus K_2$

$= 0001\ 0000\ 0110\ 1101 \oplus 1001\ 1000\ 0110\ 0101 =$

$=$

$= 1000\ 1000\ 0000\ 1000$

RSA

inverse euclidean algo.

13 d mod 60

Q	A	B	R	T_1	T_2	T
4	60	13	8	0	1	-4
1	13	8	5	1	-4	5
1	8	5	3	-4	5	-9
1	5	3	2	5	-9	14
1	3	2	1	-9	14	-23
2	2	1	0	14	-23	60
	1	0		-23	60	

$T = T1 - T2 \times Q$

$= 0 - 1 \times 4 = -4$

$T = 1 - (-4) \times 1 = 5$

$T = -4 - 5 \times 1 = -9$

$T = 5 - -9 \times 1 = 14$

$T = -9 - 14 \times 1 = -23$

$T = 14 - -23 \times 2 = 60$

$-23 \bmod 60 = 1$

$d = 60 - 23 = 37$

$p, q \rightarrow$ prime nums

$n = p \times q$

$\phi(n) = (p-1)(q-1)$

$1 < e < \phi(n)$

$\gcd(e, \phi(n)) = 1$

$e * d \bmod \phi(n) = 1 \quad , d = e^{-1} \bmod \phi(n)$

$PU = \{e, n\}$

$PR = \{d, n\}$

encrypt : $C = M^e \bmod n$

decrypt : $M = C^d \bmod n$

problems on RSA

1- $n = p \times q = 13 \times 5 = 65$

$d = e^{-1} \bmod \phi(n)$

$\phi(n) = (p-1)(q-1)$

$= 12 \times 4 = 48$

$d = 7 \times \boxed{d} \bmod 48 = 1$

$d = 7$

$c = M^e \bmod n$

$= 6^7 \bmod 65$

$6^2 \bmod 65 = 36$

$6^3 \bmod 65 = 216 \bmod 65 = 21$

$6^4 \bmod 65 = 21 \times 6 = 126 \bmod 65 = 61$

$6^5 \bmod 65 = 61 \times 6 = 366 \bmod 65 = 41$

$6^6 \bmod 65 = 41 \times 6 = 246 \bmod 65 = 51$

$6^7 \bmod 65 = 51 \times 6 = 306 \bmod 65 = 46$

$C = 46$

$n = p \times q = 5 \times 13 = 65$

$d = e^{-1} \bmod \phi(n)$

$\phi(n) = (p-1)(q-1) = 4 \times 12 = 48$

$d = 11 \times d \bmod 48 = 1$

Q	A	B	R	T_1	T_2	T	$o - 1 \times 4$
4	48	11	4	0	1	-4	
2	11	4	3	1	-4	9	$1 - -4 \times 2$
1	4	3	1	-4	9	-13	$-4 - 9 \times 1$ $-4 - 5$
3	3	1	0	9	-13	48	$9 - -9 \times 3$
	1	0		-13	48		

$-13 \bmod 48 = 1$

$d = 48 - 13 = 35$

$$PU = \{\overset{e}{11}, \overset{n}{65}\}$$

$$PR = \{\overset{d}{35}, \overset{n}{65}\}$$

encryption :

$$C = M^e \bmod n$$

$$= 5^{11} \bmod 65$$

$5^2 \bmod 65 = 25$

$5^3 \bmod 65 = 125 \bmod 65 = 60$

$5^4 \bmod 65 = 60 \times 5 = 300 \bmod 65 = 40$

$5^5 \bmod 65 = 40 \times 5 = 200 \bmod 65 = 5$

$5^{10} = (5^5)^2 = 25 \bmod 65 = 25$

$5^{11} = 5^{10} \times 5 = 125 \bmod 65 = 60$

$C = 60$

1- $n = p \times q = 11 \times 7 = 77$

$c = M^e \bmod n$

$c = 8^{17} \bmod 77$

2-

$m = c^d \bmod n$

$n = p \times q$
$= 11 \times 3 = 33$

$d = e^{-1} \bmod \phi(n)$

$d = 3^{-1} \bmod 20$

$\phi(n) = (p-1)(q-1)$
$= 10 \times 2 = 20$

$d = 7$

$M = 13^7 \bmod 33$

$13^2 \bmod 33 = 169 \bmod 33 = 4$

$13^3 = 4 \times 13 = 52 \bmod 33 = 19$

$(13^4) = (13^2)^2 = 16 \bmod 33 = 16$

$13^7 = 13^4 \times 13^3 = 16 \times 19 \bmod 33$
$= 304 \bmod 33 = 7$

$$\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}$$

$PU = \{e, n\}$

$m = 7$

$PR = \{d, n\}$

5

6

El Gamal cryptosystem

$q \rightarrow$ prime num

a or $\alpha \rightarrow a < q$

Key generation :

- select X_A $\quad X_A < q-1$
- Calculate Y_A $\quad Y_A = a^{X_A} \bmod q$
- Public key $\quad PU = \{q, a, Y_A\}$

Private key $\quad X_A$

38

1982

19x2

NATIONAL PAINTS

Encryption :

Plaintext	$M < q$
select random integer k	$k < q$
Calculate K	$K = (Y_A)^k \bmod q$
calculate C_1	$C_1 = a^k \bmod q$
Calc. C_2	$C_2 = KM \bmod q$
cipher	(C_1, C_2)

Decryption :

cipher	(C_1, C_2)
calc. K	$K = (C_1)^{X_A} \bmod q$
plaintext	$M = (C_2 K^{-1}) \bmod q$

diffie hellman

key generation:

1- Public key of A : $Y_a = a^{x_a} \bmod q$
2 public key of B : $Y_b = a^{x_b} \bmod q$

key exchange

A

- A sends Y_a to B
- B sends Y_b to A

- calc K of A $K = Y_b^{x_a} \bmod q$.
- calc K of B $K = Y_a^{x_b} \bmod q$.

Problems:

1- $q = 8$ $a = 2$ $X_a = 6$, $X_b = 0$

$R_A = a^{X_A} \bmod q = 2^6 \bmod 8$

$= 64 \bmod 8 = 0$

$R_B = b^{X_B} \bmod q = 2^0 \bmod 8 = 1$

exchange keys

$K_A = R_B^{X_A} \bmod q = 1^6 \bmod 8 = 1$

$K_B = R_A^{X_B} \bmod q = 0^0 \bmod 8$

$= 1 \bmod 8 = 1$

2- $q = 23$, $a = 5$

$X_a = 6$ $M = 9$, $K = 3$

$Y_a = a^{X_a} \bmod q = 5^6 \bmod 23$

$5^2 \bmod 23 = 2$

$5^4 \bmod 23 = 2^2 \bmod 23 = 4$

$5^6 = \cancel{5^4} \cancel{=} 4 \times 2 \bmod 23 = 8$

$K = (Y_A)^K \bmod q = 8^3 \bmod 23$

$8^2 \bmod 23 = 64 \bmod 23 = 18$

$8^3 \bmod 23 = 18 \times 8 = 144 \bmod 23$

$= 6$

$C_1 = a^k \bmod q = 5^3 \bmod 23$

$= 2 \times 5 \bmod 23 = 10$

$= 3$ $23 = 9$ 9×3 $7^4 =$

$9 \times 7 = 63$

$4 \times 4 \times 7$

$16 \times 7 = 112$

$C_2 = K \times M \mod q$

$= 6 \times 9 \mod q$

$= 54 \mod 23 = 8$

$(10, 8)$

decryption

$K = C_1^{X_a} \mod q = 10^6 \mod 23$

$10^2 \mod 23 = 100 \mod 23 = 8$

$10^4 \mod 23 = 8^2 = 64 \mod 23 = 18$

$10^6 = 10^2 \cdot 10^4 = 18 \times 8 = 144 \mod 23$

$= 6$

$-8 \bmod q =$

$19 - 8 = 11$

$= 7 \times \square \bmod 19 = 1$

$M = (C_2 K^{-1}) \bmod q$

$= 8 \times 6^{-1} \bmod 23$

$K^{-1} \bmod q = 6 \times 4 \bmod 23 = 1$

$M = 8 \times 4 \bmod 23 = 32 \bmod 23$

$= 9$

$6 \times \square \bmod 23 = 1$

4

Elliptic curve

$$y^2 = x^3 + ax + b \bmod p$$

1- point addition

$$P + Q = R$$

$$S = \frac{Y_P - Y_q}{X_P - X_q}$$

$$X_R = S^2 - (X_P + X_q)$$

$$Y_R = S(X_P - X_R) - Y_P$$

2- Point doubling

$$P = Q$$

$$P + P = 2P = R$$

$$S = \frac{3X_P^2 + a}{2Y_P}$$

$$X_R = S^2 - 2X_P$$

$$Y_R = S(X_P - X_R) - Y_P$$

3- adding vertical points in elliptic curve

$$P + Q = 0 \quad , \quad X_P = X_Q$$

Examples

$$y^2 = x^3 + 2x + 3 \bmod 17 \ , \ G = (5,1)$$

1- 2G

↳ Point doubling

$$S = \frac{3 \times 5^2 + 2}{2 \times 1} = \frac{77}{2} = 77 \times 2^{-1} \bmod 17$$

$$2 \times \square \bmod 17 = 1$$

$$= 9 \times 9 = 81 \bmod 17 = 13$$

$$X = 13^2 - 2 \times 5 = 13^2 - 10 = 169 - 10$$

$$= 159 \bmod 17 = 6$$

$$Y = S(X_P - X_R) - Y_P = 13(5-6) - 1$$

$$= -13 - 1 \bmod 17 = -14 \bmod 17$$

$$= 3$$

$2G = (6, 3)$

2 - $3G$

↳ point addition

$3G = 2G + G = (6,3) + (5,1)$

$$s = \frac{y_Q - y_P}{x_Q - x_P} = \frac{1-3}{5-6} = \frac{-2}{-1} = 2 \bmod 17 = 2$$

$x = 2^2 - (5+6) = 4 - 11 = -7 \bmod 17 = 10$

$y = \cancel{5}\ 2(6-10) - 3 = \overset{-11}{-8} - 3 \bmod 17 = 6$

$3G = (10, 6)$

2 - $y^2 = x^3 + 2x + 3 \bmod 17$ $P = (5, 11)$

1-2P → doubling

$$s = \frac{3 \times 5^2 + 2}{2 \times 11} = \frac{77}{22} \bmod 17 = 77 \times 22^{-1} \bmod 17$$

$= 9 \times 7 \bmod 17 = 63 \bmod 17 = 12$

$X = 12^2 - 2 \times 5 = 144 - 10 = 134 \bmod 17 = 15$

$Y = 12 \times (5 - 15) - 11 = -120 - 11 = -131$

$-131 \bmod 17 = -12 \bmod 17 = 5$

$2P = (15, 5)$

$P_2 = (5, 11)$ $P_1 = (15, 5)$

$3P = 2P + P$ → addition

$$\delta = \frac{y_2 - y_1}{x_2 - x_1} = \frac{11 - 5}{5 - 15} = \frac{6}{-10} \bmod 17$$

$= 13$

$$x = 13^2 - 15 - 5 = 169 - 20 = 149 \bmod 17$$
$$= 13$$

$$y = 13(15 - 13) - 5 = 21 \bmod 17 = 4$$

$3P = (13, 4)$