HW#1

1. (1) $(X_1\ X_2\ X_3\ X_4\ X_5\ X_6) = (0, 19, 19, 0, 2, 10)$

$y_1 = 9 \cdot 0 + 13 \mod 26 = 13$

$y_2 = 9 \cdot 19 + 13 \mod 26 = 184 \mod 26 = 2$.

$\vdots$

$(y_1, y_2, y_3, y_4, y_5, y_6) = (13, 2, 2, 13, 5, 25) = \text{nccnfz}$.

(2) $a \cdot a^{-1} \equiv 1 \mod 26$

$3 \cdot 9 = 27 \equiv 1 \mod 26 \quad \therefore a^{-1} = 3$

$x_1 = 3(13-13) \mod 26 = 0$

$x_2 = 3(2-13) \mod 26 = -33 \mod 26 = 19 \mod 26$

$x_5 = 3(5-13) \mod 26 = -24 \mod 26 = 2$

$x_6 = 3(25-13) \mod 26 = 36 \mod 26 = 10$

$(x_1, x_2, x_3, x_4, x_5, x_6) = (0, 19, 19, 0, 2, 10)$

(3) key space = (# value for a) × (# values for b)

$= 12 \times 26 = \underline{312}$.

since $\gcd(a, 26) = 1$

$\rightarrow a \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

2. (1) Feistel cipher

$P = (L_0, R_0)$

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

$F(R_{i-1}, K_i) = K_i$

$L_1 = R_0$

$R_1 = L_0 \oplus K_1$

$L_2 = R_1 = L_0 \oplus K_1$

$R_2 = L_1 \oplus K_2 = R_0 \oplus K_2$

$L_3 = R_2 = R_0 \oplus K_2$

$R_3 = L_2 \oplus K_3 = L_0 \oplus K_1 \oplus K_3$

$L_4 = R_3 = L_0 \oplus K_1 \oplus K_3$

$R_4 = L_3 \oplus K_4 = R_0 \oplus K_2 \oplus K_4$

$\therefore (L_4, R_4) = (L_0 \oplus K_1 \oplus K_3,\ R_0 \oplus K_2 \oplus K_4)$

(2) $F(R_{i-1}, K_i) = R_{i-1} \oplus K_i$

$L_1 = R_0$
$R_1 = L_0 \oplus R_0 \oplus K_1$

$L_2 = R_1 = L_0 \oplus R_0 \oplus K_1$
$R_2 = L_1 \oplus R_1 \oplus K_2 = R_0 \oplus L_0 \oplus R_0 \oplus K_1 \oplus K_2 = L_0 \oplus K_1 \oplus K_2$

$L_3 = R_2 = L_0 \oplus K_1 \oplus K_2$
$R_3 = L_2 \oplus R_2 \oplus K_3 = \cancel{L_0} \oplus R_0 \oplus \cancel{K_1} \oplus \cancel{L_0} \oplus \cancel{K_1} \oplus K_2 \oplus K_3$
$= R_0 \oplus K_2 \oplus K_3$

$L_4 = R_3 = R_0 \oplus K_2 \oplus K_3$
$R_4 = L_3 \oplus R_3 \oplus K_4 = L_0 \oplus K_1 \oplus \cancel{K_2} \oplus R_0 \oplus \cancel{K_2} \oplus K_3 \oplus K_4$
$= L_0 \oplus R_0 \oplus K_1 \oplus K_3 \oplus K_4$

$C = (L_4, R_4) = (R_0 \oplus K_2 \oplus K_3, L_0 \oplus R_0 \oplus K_1 \oplus K_3 \oplus K_4)$

HW # 2.

1. ① random number
   ② timestamp
   ③ some IDs, IP address, etc.

2. Errors on one block of the ciphertext do not influence the following blocks of the ciphertext.
   (But, it is ~~not~~ the case on errors on the plaintext blocks.)

3. (a) encryption

$$C = 19^3 \bmod 33 = 28$$

   (b) decryption

$$m = 28^7 \bmod 33 = 19$$

HW #3

1. $a = 6$

$a^1 = 6 \bmod 11 = 6$

$a^2 = 36 \bmod 11 = 3$

$a^3 = 3 \times 6 \bmod 11 = 7$

$a^4 = 7 \times 6 \bmod 11 = 9$

$a^5 = 9 \times 6 = 54 \bmod 11 = 10$

$a^6 = 10 \times 6 = 60 \bmod 11 = 5$

$a^7 = 5 \times 6 = 30 \bmod 11 = 8$

$a^8 = 8 \times 6 = 48 \bmod 11 = 4$

$a^9 = 4 \times 6 = 24 \bmod 11 = 2$

$a^{10} = 2 \times 6 = 12 \bmod 11 = 1$

$a^{11} = 1 \times 6 = 6 \bmod 11 = 6$

$\therefore$ order $= 10$.

2. $E : y^2 = x^3 + 7x + b \pmod{11}$

$P \in (4,5) \Rightarrow b = ?$

$5^2 = 4^3 + 7 \times 4 + b \pmod{11}$

$25 = 64 + 28 + b \pmod{11}$

$3 = 9 + 6 + b \pmod{11}$

$= 4 + b \pmod{11}$

$\therefore b = 10$

List all points on E.

$x = 0 \rightarrow y^2 = 10 \bmod 11 \Rightarrow y =$ none.

$x = 1 \rightarrow y^2 = 1 + 7 + 10 \pmod{11} = 7 \bmod 11 \Rightarrow$ none

$x = 2 \rightarrow y^2 = 8 + 14 + 10 \pmod{11} = 10 \bmod 11 \Rightarrow$ none

$x = 3 \rightarrow y^2 = 27 + 21 + 10 \pmod{11} = 5 + 10 + 10 \pmod{11}$

$= 3 \bmod 11$

$y^2 = 25 \rightarrow y = 5$ $\quad$ (3,5)

$y^2 = 36 \rightarrow y = 6$ $\quad$ (3,6)

$x = 4 \rightarrow y^2 = 64 + 28 + 10 \pmod{11}$

$= 3 \bmod 11 \Rightarrow$ (4,5), (4,6)

$x = 5 \rightarrow y^2 = 125 + 35 + 10 \pmod{11}$

$= 16 \pmod{11} = 5 \bmod 11$

$\Rightarrow y^2 = 16 \Rightarrow y = 4$ $\quad$ (5,4)

$= 36 \Rightarrow y = 6$ $\quad$ (5,6)

$X=6 \rightarrow y^2 \equiv 216+42+10 \pmod{11}$

$= 7+9+10 \pmod{11}$

$= 4 \bmod 11$

$\Rightarrow y^2 = 4 \rightarrow y=2 \quad \boxed{(6,2)}$

$=81 \quad \boxed{(6,9)}$

therefore, $\{(3,5)(3,6)(4,5)(4,6)(5,4)(5,6)(6,2)(6,9)\}$

$(4,5)+(5,4) = (x_3, y_3)$

$m = (4-5)(5-4)^{-1} \bmod 11$

$= (-1)(1)^{-1} \bmod 11$

$= 10 \cdot 1 \bmod 11$

$= 10 \bmod 11$

$x_3 = 10^2 - 4 - 5 \pmod{11}$

$= 91 \bmod 11 = 3 \bmod 11$

$y_3 = 10(4-3) - 5$

$= 5 \bmod 11$

$\therefore (x_3, y_3) = (3,5)$

3. (a) sign $s = M^d \bmod 33$

$= 25^7 \bmod 33 = 31$

(b) verify $M' = s^e \bmod 33$

$= 31^3 \bmod 33 = 25 = M$

4. $p=23,\ d=9,\ g=5,\ x=10$

select $k_E = 7 \in Z_{22}$ s.t. $\gcd(7,22)$

$k_E^{-1} = 19 \bmod 22$

(a) sign $r = 5^7 \bmod 23 = \boxed{17} \bmod 23$

$s = (10 - 9 \cdot 17) \cdot 7^{-1} \bmod 22 = \boxed{11} \bmod 22$

Alice $\xrightarrow{(10, (17, 22))}$ Bob

(b) verify $v = \beta^r r^s \bmod p$

$= 11^9 \cdot 17^{11} \bmod 23$

$= 5^{10} \bmod 23$

$v' = g^x \bmod p = 5^{10} \bmod 23$

$\left(\beta = g^d \bmod p = 5^9 \bmod 23 = 11 \bmod 23\right)$

$\therefore v = v'$

5. $p=27$, $q=13$, $x=5$, $H(x)=5$

choose $g=6$ s.t. $g^q=1 \bmod p$. ($\gcd(g,p)=1$)

choose $d=7$.

(a) select $k=2$, $k^{-1} \bmod q = 2^{-1} \bmod 13 = 7$

$$r = (g^k \bmod p) \bmod q$$
$$= (6^2 \bmod 27) \bmod 13$$
$$= \boxed{9} \bmod 13$$
$$s = k^{-1}(H+d\cdot r) \bmod q$$
$$= 2^{-1}(5+7\cdot 9) \bmod 13$$
$$= 7\cdot 68 \bmod 13$$
$$= 7\cdot 3 \bmod 13$$
$$= \boxed{8}$$

(b) verify

$$s' = 8^{-1} \bmod 13 = \boxed{5} \bmod 13$$
$(8\cdot 8^{-1} \bmod 13 = 1 \bmod 13)$

$$r' = (\beta^{s'r} g^{s'H'} \bmod p) \bmod q$$
$$= (\beta^{5\times 9} 6^{5\times 5} \bmod 27) \bmod 13$$

check $r' \stackrel{?}{=} 9$

6. (a) The computed MAC is different from the MAC received.

(b) So far, there is no known ~~attl~~ attacks.

So, the lesson is that the keys for encryption and MAC should be different. But two keys may be related in some ways. (Two keys are allowed to have some relations.)

9. input : $(Tlen, k, k_1, M=(\underbrace{M_1, \cdots, M_N}_{M[1, \cdots, N]}), N \text{ blocks})$

output : h

{ $C[1] \leftarrow E_k(M[1])$

$i \leftarrow 2$

while $(i < N)$

$C[i] \leftarrow E_k(C[i-1] \oplus M[i])$

$i \leftarrow i+1$

$C[N] \leftarrow E_k(C[N-1] \oplus M[N] \oplus k)$

$h \leftarrow$ selectLeft$(C[N], Tlen)$

return h

}