Midterm 1　　游鎮遠 111061548

1. Ans: public-key, advantages: (i) High security
(ii) Convenience
(iii) Asymmetry

, disadvantages: (i) Low-efficency
(ii) Reliability

symmetric-key, advantages: (i) High-efficency
(ii) Reliability

, disadvantages: (i) key distribution
(ii) Lower security

2. Ans: $A \preceq_{poly} B$

* if there is a poly-time algorithm C for solving B, there is another poly-time algorithm H for solving A.
* An instance of A can be transformed into an instance of B.
* the same meaning: (i) Reduce A to B.
(ii) B is reduced to A

3. Ans:

The adversary knows all details about a cryptosystem except the used private keys.

4. DES - CFB

DES used 64-bits to generate keys, and it self-synchronized after $\lceil \frac{n}{s} \rceil$ if an entire block is lost.

m_i is 16-bits long.

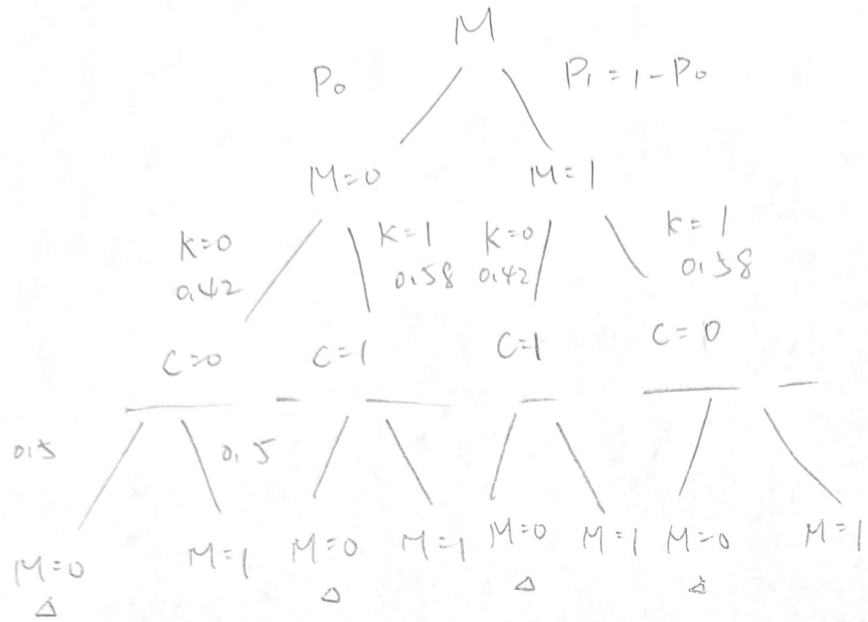
$$\lceil \frac{64}{16} \rceil = 4$$

so wrong will be affected $m_9 \sim m_{13}$, $m_{16} \sim m_{20}$, $m_{26} \sim m_{30}$, $m_{89} \sim m_{93}$.

#

5. (a)

Ans: $Pr[M=b] = P_b$, $b \in [0,1]$, $Pr[K=0] = 0.42$, $Pr[K=1] = 0.58$



$Pr[M=0]$

$= P_0 \times 0.42 \times 0.5 + P_0 \times 0.58 \times 0.5 + (1-P_0) \times 0.42 \times 0.5 + (1-P_0) \times 0.58 \times 0.5$

$= 0.5 P_0 (0.42 + 0.58) + 0.5 (1-P_0) (0.42 + 0.58)$

$= 0.5 (P_0 + 1 - P_0) = 0.5$ #

5. (b)

Ans:

$$Pr[M=0 \mid C=0] = \frac{Pr[C=0 \mid M=0] \times Pr[M=0]}{Pr[C=0]}$$

$$= \frac{0.42 P_0}{0.42 P_0 + 0.58 P_1}$$

$$Pr[M=0 \mid C=1] = \frac{0.58 P_0}{0.58 P_0 + 0.42 P_1}$$

$$Pr[M=1 \mid C=0] = \frac{0.58 P_1}{0.42 P_0 + 0.58 P_1}$$

$$Pr[M=1 \mid C=1] = \frac{0.42 P_1}{0.58 P_0 + 0.42 P_1}$$

When $c=0$, if $0.42P_0 > 0.58P_1$, A_2 guess $M=0$.

elif $0.42P_0 < 0.58P_1$, A_2 guess $M=1$

when $c=1$, if $0.58P_0 > 0.42P_1$, A_2 guess $M=0$,

elif $0.58P_0 < 0.42P_1$, A_2 guess $M=1$

#

6.

$$\begin{cases} x \bmod 7 = 1 \\ x \bmod 15 = 1 \\ x \bmod 17 = 12 \end{cases}$$

Ans:

$$x = (1\times 15\times 17\times (15\times 17)^{-1} \bmod 7 + 3\times 7\times 17\times (7\times 17)^{-1} \bmod 15 + 17\times 12\times 15\times (17\times 15)^{-1} \bmod 17) \bmod 1785$$

$$7\times 15\times 17 = 1785$$

$M_1 = 255$, $M_2 = 119$, $M_3 = 105$

$$\begin{cases} 255 \bmod 7 = 3, \quad 3\times 5 = 15 \bmod 7 = 1 \\ 119 \bmod 15 = 14, \quad 14\times 14 = 196 \bmod 15 = 1 \\ 105 \bmod 17 = 3, \quad 3\times 6 = 18 \bmod 17 = 1 \end{cases}$$

$$\therefore \begin{cases} (15\times 17)^{-1} \bmod 7 = 5 \\ (7\times 17)^{-1} \bmod 15 = 14 \\ (7\times 15)^{-1} \bmod 17 = 6 \end{cases}$$

$\Rightarrow x = 1338$ #

7. $f(x) = x^{-1} \bmod X^8+X^4+X^3+X+1$,

$f(01100011)$ is X^6+X^5+X+1 under $GF(2^8)$

Ans: compute $\gcd(X^8+X^4+X^3+X+1,\ X^6+X^5+X+1)$

$$X^8+X^4+X^3+X+1 = (X^6+X^5+X+1)\times(X^2+X+1) + (X^5+X^4+X)$$
$$X^6+X^5+X+1 = (X^5+X^4+X)\times X + (X^2+X+1)$$
$$X^5+X^4+X = (X^2+X+1)\times(X^3+X+1) + (X+1)$$
$$X^2+X+1 = (X+1)\times X + 1$$

---

let $A = X^8+X^4+X^3+X+1$

$B = X^6+X^5+X+1$, $C = X^5+X^4+X = A-B(X^2+X+1)$

$1 = (X^2+X+1) - (X+1)X$

$= (B-CX) - (C-(B-CX)(X^3+X+1))X$

$= (B-CX) - (C-BX^3+BX+B+CX^4+CX^2+CX)X$

$= B+CX+CX+BX^4+BX^2+BX+CX^5+CX^3+CX^2$

$= B(X^4+X^2+X+1) + C(X^5+X^3+X^2)$

$= B(X^4+X^2+X+1) + (A-B(X^2+X+1))(X^5+X^3+X^2)$

$= A(X^5+X^3+X^2) + B((X^4+X^2+X+1)+(X^2+X+1)(X^5+X^3+X^2))$

$= A(X^5+X^3+X^2) + B(X^4+X^2+X+1+X^7+X^5+X^4+X^6+X^4+X^3+X^2+X^3+X^2)$

$= A(X^5+X^3+X^2) + B(X^7+X^6+X^4+X+1)$

$\therefore f(01100011) = 11010011$ #