# Solutions

2021年4月22日　　上午 08:53

1.

| $i$ | $r_i$ | $q_i$ | $x_i$ | $y_i$ |
|---|---|---|---|---|
| -1 | 184 | | 1 | 0 |
| 0 | 57 | 3 | 0 | 1 |
| 1 | 13 | 4 | 1 | -3 |
| 2 | 5 | 2 | -4 | 13 |
| 3 | 3 | 1 | 9 | -29 |
| 4 | 2 | 1 | -13 | 42 |
| 5 | 1 | | 22 | -71 |

$x$　$y$

2. By the CRT formula,

$$x = [\,2\cdot(7\cdot13)\,((7\cdot13)^{-1} \bmod 6) + 4\,(6\cdot13)\,((6\cdot13)^{-1} \bmod 7) + 1\,(6\cdot7)\,((6\cdot7)^{-1} \bmod 13)\,] \bmod 6\cdot7\cdot13$$

$$= 326$$

3. By the Euclidean algorithm:

$2x^2+x+5$ or $a\cdot(2x^2+x+5)$, $a \in \mathbb{Z}_7^*$

$$\rightarrow \begin{cases} 4x^2+2x+3 & a=2 \\ 6x^2+3x+1 & a=3 \\ x^2+4x+6 & a=4 \\ 3x^2+5x+4 & a=5 \\ 5x^2+6x+2 & a=6 \end{cases}$$

4.

$a = 37_H = 0011\ 0111$

$b = A6 = 1010\ 0110$

| $i$ | $b_i$ | $f$(shift-xor) | $f$(mod $g(x)$) |
|---|---|---|---|
| 0 | | 0000 0000 | 0000 0000 |
| 7 | 1 | 0011 0111 | 0011 0111 |
| 6 | 0 | 0110 1110 | 0110 1110 |
| 5 | 1 | 1110 1011 | 1110 1011 |
| 4 | 0 | 1101 0110 | 1100 1101 |
| 3 | 0 | 1001 1010 | 1000 0001 |

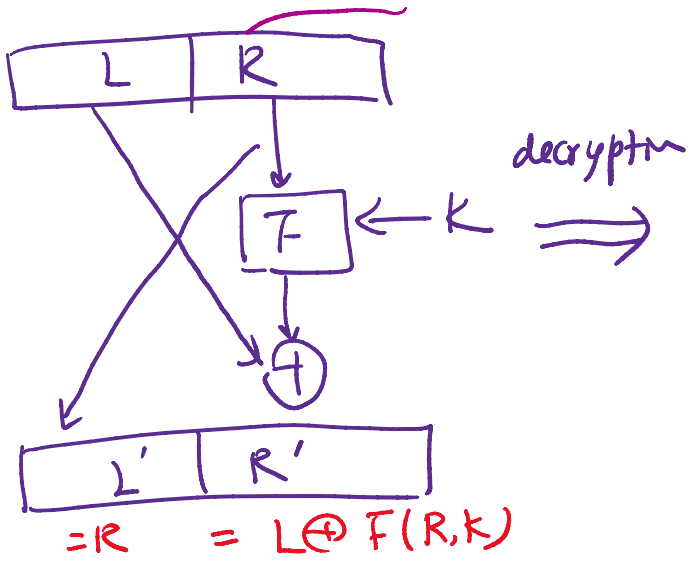
| | | | |
|---|---|---|---|
| 4 | 0 | 1101 0110 | 1100 1101 |
| 3 | 0 | 1001 1010 | 1000 0001 |
| 2 | 1 | 1011 0101 | 0010 1110 |
| 1 | 1 | 0110 1011 | 0110 1011 |
| 0 | 0 | 1101 0110 | 1101 0110 |

D 6

5. Add Roundkey → substitution
Sub Byte → substitution
Shift Row → permutation
Mix Column → substitution

Explanation can be found in class slides

6.




=R = L⊕F(R,K)

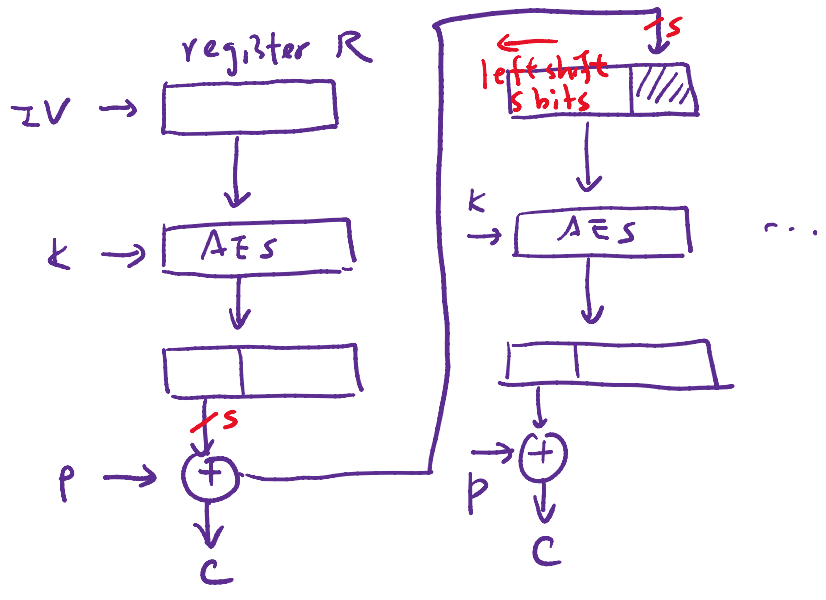
=R = L⊕F(R,K)⊕F(L',K)

= L⊕F(R,K)⊕F(R,K)

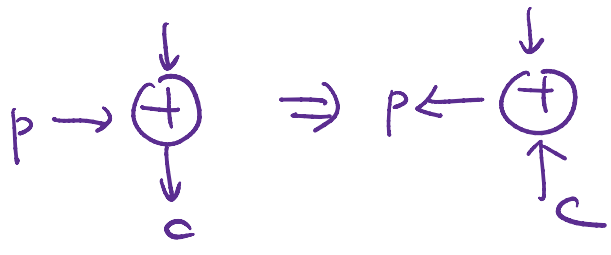
= L

Thus, no matter what F is, L can be recovered.

7. (a)




Decryption: the same except that



(b) Since an erroneous ciphertext of 5 bytes would stay in register R for $\lceil \frac{16}{5} \rceil$ blocks in decryption, the next $\lceil \frac{16}{5} \rceil$ blocks of decryption are wrong.

So, $P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}$ and

$P_{83}$ $P_{84}$ $P_{85}$ $P_{86}$ $P_{87}$ $P_{88}$ $P_{89}$ are decrypted incorrectly.

8. (a) $\varphi(n) = (11-1)(13-1) = 120$

$d = e^{-1} \bmod \varphi(n) = 7^{-1} \bmod 120 = 103$

(b) (i) m "mod 11" space.

$C' = C \bmod 11 = 8$

$d' = d \bmod (11-1) = 3$

$m' = (C')^{d'} \bmod 11 = 8^3 \bmod 11 = 6$

(ii) m "mod 13" space

$C'' = C \bmod 13 = 8$

$d'' = d \bmod (13-1) = 7$

$m'' = (C'')^{d''} \bmod 13 = 8^7 \bmod 13 = 5$

Then, by CRT

$$m = (6 \cdot 13 \cdot (13^{-1} \bmod 11) + 5 \cdot 11 (11^{-1} \bmod 13)] \bmod 143$$

$$= (6 \cdot 13 \cdot 6 + 5 \cdot 11 \cdot 6) \bmod 143$$

$$= 83$$

(c) Case I: $M \perp n$,

$$C^d \bmod n = M^{ed} \bmod n = M^{k \cdot \phi(n)} \cdot M \bmod n$$

$$= ((M^{\phi(n)} \bmod n)^k \cdot M) \cdot \bmod n$$

$$= (1^k \cdot M) \bmod n$$

By Euler's theorem: $M^{\phi(n)} \bmod n = 1$ since $M \perp n$.

Case II: $\gcd(M, n) \neq 1$

assume that $M = aP$, $0 \le a < q-1$

let $x = C^d \bmod n$.

We have

$x \bmod P = 0 = M \bmod P = r_1$

We have

(i) $x \bmod p = 0 = M \bmod p = r_1$

(ii) $x \bmod q = M^{k\cdot(p-1)(q-1)+1} \bmod q$

$= \left(M^{q-1} \bmod q\right)^{k\cdot(p-1)} \cdot M \bmod q$ ← since $M \perp q$.

$= 1^{k\cdot(p-1)} \cdot M \bmod q$ ← $M^{q-1} \bmod q = 1$ by Fermat's little theorem

$= M \bmod q = r_2$

By CRT, there is a unique solution $x_0$, $0 \le x_0 \le n-1$

for the equations: $x \bmod p = r_1 = 0$, $x \bmod q = r_2 = M \bmod q$.

Since $M \bmod p = r_1$ and $M \bmod q = r_2$, $M$ is a solution in $(0, n-1]$

Thus, $x = M$.