列印成品

2024年4月12日　　下午 12:48

Introduction to Cryptography, 2024 Spring

Midterm, 4/12/2024 (Friday)

1. Consider the affine cipher whose encryption function is $E([a, c], m) = (a \times m + c) \bmod 26$, which encrypts English character $m \in \{0, 1, 2, ..., 25\}$ with key [a, c], where $0 \le a, c \le 25$.

   (a) (5%) How many legal keys are there for the affine cipher?

   (b) (5%) Explain the criteria for a key to be legal.

2. (10%) Solve the equation $183x + 76y = 1$ for integers x and y by filling out the following table with the extended Euclidean algorithm, where $183x_i + 76y_i = r_i$ for all $i \ge -1$
   Note: No credits if any error occurs in the table.

i	r_i	q_i	x_i	y_i
-1	183		1	0
0	76		0	1
1	...	...	...	...
...	...	...	...	...

3. (10%) AES's byte operations are defined on the finite field $GF(2^8)/x^8 + x^4 + x^3 + x + 1$. Use the Shift-XOR-Mod algorithm to compute $7A \times D3$ by filling out the following table.
   Note: No credits if any error occurs in the table.

i	b_i	f (shift-XOR)	f (mod g(x))
		0000 0000	0000 0000
7	1	...	...
...	...	...	...

4. (10%) Use the CRT number system mapping to compute $a = 3^{1882} \bmod 117$ with detailed steps.
   Note: use trials to find modular inverses. No credits if using other methods or not writing the correct CRT formula.

5. Use the baby-step-giant-step algorithm to compute $x = \text{dlog}_{11,29}13$ by the following steps:

   (a) (5%) Build the tables for (j, b_j) and (i, a_i), $0 \le i, j \le m - 1$

   (b) (5%) Compute all possible x by the above tables, $0 \le x \le 28$
   Note: no credits if (a) is wrong.

6. Consider the AES input plaintext 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F (Hex).

   (a) (5%) What is the state array after applying the ShiftRows function on the state array from the input plaintext?

   (b) (5%) What is the second column of the state array after applying the MixColumns function on the state array from (a)?
   Note: MixColumns multiplies the columns of state array by $03y^3+01y^2+01y+02 \bmod 01y^4+01$. No credits if (a) is wrong.

(see next page)

7. Let the left and right parts of the Feistel structure input be L and R and the used function be F.

   (a) (5%) What are the left and right parts L' and R' of the Feistel structure output?

   (b) (5%) Show that if R' and L' are used as the left and right parts of the Feistel structure input, the output is R and L no matter what F is.
   Note: no credits if (a) is wrong.

8. Alice uses AES in CFB mode to encrypt a message of 20-bit block size to Bob, that is, the feedback size is 20 bits.

   (a) (5%) Describe the encryption diagram of AES in the CFB mode of 20-bit feedback.

   (b) (5%) Bob received ciphertext blocks C_1 $C_2 \ldots$ C_{100} and decrypted to get message blocks M_1 $M_2 \ldots$ M_{100}. By the embedded error detecting code used in transmission, Bob knew that there are bit errors in C_5 and a missing block between C_{65} and C_{66}. What message blocks should be discarded by Bob?
   Note: no credits if (a) is wrong.

9. Alice wants to send a ciphertext to other people by the Vernam cipher and uses the LFSR $B_3X + B_1X^3 + B_0X^4$ as the key stream generator.

   (a) (5%) What is the generated bit sequence of 12 bits if the seed of the LFSR is $B_3B_2B_1B_0 = 0011$?

   (b) (5%) Alice sends the ciphertext C_1 = 1000 1001 0110 1100 to Bob and notifies Bob the used seed in the LFSR. She also sends the ciphertext C_2 = 1000 0101 0110 1011 to Carol and notifies Carol the used seed. Eve knew that Alice uses the same seed for C_1 and C_2. She also knew that the sent messages to Bob and Carol are the ASCII codes of two digits, d_1d_2 to Bob and e_1e_2 to Carol. What information about d_1d_2 and e_1e_2 can Eve infer by the obtained information?
   Note: the ASCII code for digits are '0' → 30 (Hex), '1' → 31 (Hex), ... '9'→ 39 (Hex)

10. Consider the one-time pad cipher of encrypting n-bit messages, where an n-bit key is chosen uniformly. Assume that the message has distribution $\Pr[M = m] = p_m, m \in \{0,1\}^n$. Show that the posterior distribution of M after observing a ciphertext $c \in \{0,1\}^n$ is not altered by the following steps:

    (a) (5%) Compute $\Pr[C = c]$ for $c \in \{0,1\}^n$

    (b) (5%) Compute $\Pr[M = m | C = c]$ for $m, c \in \{0,1\}^n$

    Note: you need to write correct probability formulae before computation. Otherwise, no credits.

Solutions

1. (a) For a key $[a,c]$ to be legal, $E([a,c],m)$ must be one to one,

that is, $m_1 \neq m_2 \Rightarrow E([a,c],m_1) \neq E([a,c],m_2)$

$\Rightarrow a m_1 + c \bmod 26 \neq a m_2 + c \bmod 26$

$\Rightarrow a(m_1 - m_2) \bmod 26 \neq 0$ for $m_1 \neq m_2$

$\Rightarrow \gcd(a, 26) = 1$.

Thus, there are $|Z_{26}^*| \times 26 = 312$

(b) $\gcd(a, 26) = 1$.

2.

i	r_i	q_i	x_i	y_i
-1	183		1	0
0	76		0	1
1	31	2	1	-2
2	14	2	-2	5
3	3	2	5	-12
4	2	4	-22	53
5	1	1	27	-65

$\Rightarrow x = 27, y = -65$

3. $7A = 0111\ 1010$ $D3 = 1101\ 0011$ $g(x) = 1\,0001\,1011$

i	b_i	f (s-XOR)	$f \pmod{g(x)}$
		0000 0000	0000 0000
7	1	0111 1010	0111 1010
6	1	1000 1110	1000 1110
5	0	1\,0001 1100	0000 0111
4	1	0111 0100	0111 0100
3	0	1110 1000	1110 1000
2	0	1\,1101 0000	1100 1011
1	1	1\,1110 1100	1111 0111

1	1	1 1110 1100	1111	0111
0	1	1 1001 0100	1000	1111
			8	F

4. $a = 3^{1882} \bmod 117$

Since $117 = 9 \times 13$ and $\gcd(9, 13) = 1$.

Use CRT number system mapping: $Z_{117} \longleftrightarrow Z_9 \times Z_{13}$

$a \to (a \bmod 9,\ a \bmod 13)$ → $3^{1882} \bmod 117 \bmod 13 = 3^{1882 \bmod 12} \bmod 13$

$= (0, 3)$ $= 3^{10} \bmod 13 = 3$

$\to [0 \cdot 13 \times (13^{-1} \bmod 9) + 3 \cdot 9 \cdot (9^{-1} \bmod 13)] \bmod 117$

$= (0 + 3 \cdot 9 \cdot 3) \bmod 117$

$= 81$

5. (a) $m = \lceil \sqrt{29} \rceil = 6$, $11^{-6} \bmod 29 = 8^6 \bmod 29 = 13$

j	$b_j = g^j \bmod 29$	i	$a_i = y \cdot (g^{-6})^i \bmod p$
0	1	0	13
1	11	1	24
2	5	2	22
3	26	(3)	25
(4)	25	4	6
5	14	5	20

(b) $y = 3 \cdot m + 4 \bmod 28 = 22$

6. (a) plaintext → state array → shiftrows

00	04	08	0C
01	05	09	0D
02	06	0A	0E
03	07	0B	0F

→

00	04	08	0C
05	09	0D	01
0A	0E	02	06
0F	03	07	0B

(b) $(03y^3 + 0Ey^2 + 09y + 04) \times (03y^3 + 01y^2 + 01y + 02) \bmod 01y^4 + 01$

$= (03 \times 02 + 0E \times 01 + 09 \times 01 + 04 \times 03) y^3$

$+ (03 \times 03 + 0E \times 02 + 09 \times 01 + 04 \times 01) y^2$

$+ (03 \times 01 + 0E \times 03 + 09 \times 02 + 04 \times 01) y$

$+ (03 \times 01 + 0E \times 01 + 09 \times 03 + 04 \times 02)$

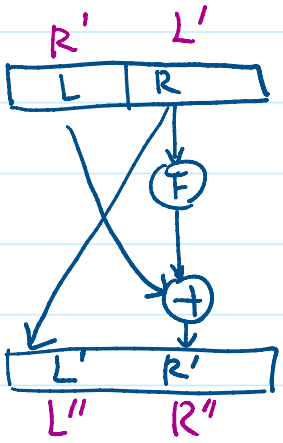
$= (06 + 0E + 09 + 0C) y^3 + (05 + 1C + 09 + 04) y^2$

$(03 + 12 + 12 + 04) y + (03 + 0E + 1B + 08)$

$= (0D) y^3 + (14) y^2 + (07) y^1 + 1E$

7.

(a)



$L' = R$

$R' = L \oplus F(R)$

(b) $L'' = L' = R$

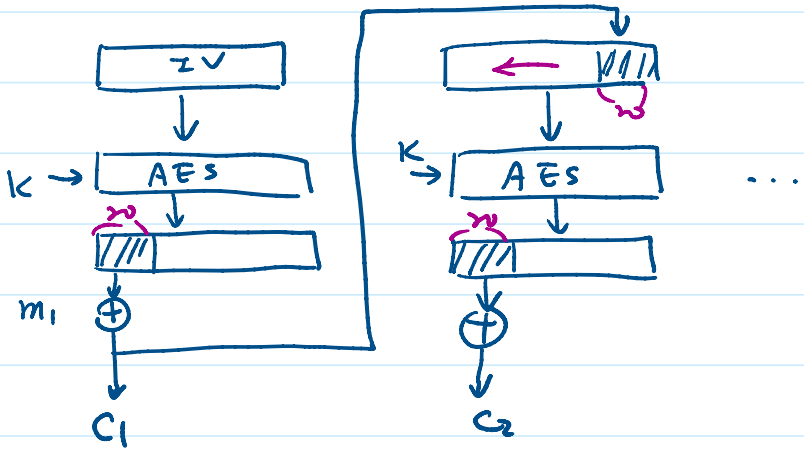
$R'' = R' \oplus F(L')$

$= L \oplus F(R) \oplus F(R)$

$= L.$

Thus, the output is R, L no matter what F is.

8. (a)



(b) C_5 is wrong $\Rightarrow$ cause subsequent $\lceil \frac{28}{20} \rceil = 7$ blocks wrong

$\Rightarrow m_5 \underline{m_6 \cdots m_{12}}$ are wrong.

C_{65} $\square$ C_{66} $\Rightarrow$ $\bar{C}_{65}$ $C_{66} \cdots C_{90}\, C_{91}$ is wrong for m_{92}

missed $\bar{C}_{65}$ $C_{66}\, C_{67}\, C_{68} \cdots C_{92}$ is correct for m_{93}

$\Rightarrow m_{66} \sim m_{92}$ are wrong

9. (a)

B_3	B_2	B_1	B_0	output
0	0	1	1	1
0	0	0	1	1
1	0	0	0	0
1	1	0	0	0
1	1	1	0	0
0	1	1	1	1
0	0	1	1	1
0	0	0	1	1
1	0	0	0	0
1	1	0	0	0
1	1	1	0	0
0	1	1	1	1

$B_3 \oplus B_1 \oplus B_0 \rightarrow$

period

repeated period

$\Rightarrow$ output ...

* 0 | | | 1

⇒ output 110001 110001

(b) The keys are the same for C_1 and C_2.

This $C_1 \oplus C_2 = [d_1 d_2 \oplus K] \oplus (e_1 e_2 \oplus K)$

$= d_1 d_2 \oplus e_1 e_2$

$= (d_1 \oplus e_1)(d_2 \oplus e_2)$

$= 0000\ 1100\ 0000\ 0111$

possible (d_1, e_1) = ('9','5'), ('8','4'), ('5','9'), ('4','8')

⇒ possible (d_2, e_2) = ('7','0'), ('0','7'), ('6','1'), ('1','6'), ('5','2'), ('2','5'), ('4','3'), ('3','4')

(a) $Pr[C=c] = \sum_m Pr[C=c \mid M=m] \cdot Pr[M=m]$

$= \sum_m Pr[K = c \oplus m \mid M=m] \cdot Pr[M=m]$

$= \sum_m \frac{1}{2^n} \cdot Pr[M=m]$

$= \frac{1}{2^n}$

(b) $Pr[M=m \mid C=c] = Pr[C=c \mid M=m] \cdot Pr[M=m] / Pr[C=c]$

$= Pr[K = c \oplus m \mid M=m] \cdot Pr[M=m] / 1/2^n$

$= (1/2^n) \cdot Pr[M=m] / \frac{1}{2^n}$

$= Pr[M=m]$

↳ not changed for any $c \in \{0,1\}^n$