1172/DCP1323 Introduction to Cryptography, Spring 2019 **Due: 2019/4/22 (Mon.)**

Homework 4

Instructor: Prof. Wen-Guey Tseng Scribe: Jeffrey Ping

1. If we take the linear congruential algorithm with an additive component of 0,

$$X_{n+1} = (aX_n) \bmod m$$

Then it can be shown that if m is prime and if a given value of a produces the maximum period of m - 1, then a^k will also produce the maximum period, provided that k is less than m and that k and m - 1 are relatively prime. Demonstrate this by using $X_0 = 1$ and m = 31 and producing the sequences for $a^k = 3, 3^2, 3^3$, and 3^4.

answer.

k = 1: 1, 3, 9, 27, 19, 26, 16, 17, 20, 29, 25, 13, 8, 24, 10, 30, 28, 22, 4, 12, 5, 15, 14, 11, 2, 6, 18, 23, 7, 21, 1

k = 2: 1, 9, 19, 16, 20, 25, 8, 10, 28, 4, 5, 14, 2, 18, 7, 1

k = 3: 1, 27, 16, 29, 8, 30, 4, 15, 2, 23, 1

k = 4: 1, 81, 20, 8, 28, 5, 2, 7, 9, 16, 25, 10, 4, 14, 18, 1

2. Alice and Bob agree to communicate privately via email using a scheme based on RC4, but they want to avoid using a new secret key for each transmission. Alice and Bob privately agree on a 128-bit key k. To encrypt a message m, consisting of a string of bits, the following procedure is used.

1. Choose a random 64-bit value v
2. Generate the ciphertext c = RC4(v || k) ⊕ m
3. Send the bit string (v || c)

a. Suppose Alice uses this procedure to send a message m to Bob. Describe how Bob can recover the message m from (v || c) using k.

answer.

m = RC4(v || k) ⊕ c

b. If an adversary observes several values (v1 || c1), (v2 || c2), c transmitted between Alice and Bob, how can he/she determine when the same key stream has been used to encrypt two messages?

answer.

c1 ⊕ c2 = (m1 ⊕ RC4(v1 || k)) ⊕ (m2 ⊕ RC4(v2 || k)) = …?

c. Approximately how many messages can Alice expect to send before the same key stream will be used twice? Use the result from the birthday paradox described in Appendix U.

answer.

Since the key is fixed, the key stream varies with the choice of the 64-bit v, which is selected randomly. Thus, after approximately $\sqrt{\frac{\pi}{2}2^{64}} \approx 2^{32}$ messages are sent, we expect the same v, and hence the same key stream, to be used more than once.

d. What does this imply about the lifetime of the key k (i.e., the number of messages that can be encrypted using k)?

answer.

The key k should be changed sometime before 2^{32} messages are sent.

3. Suppose you have a true random bit generator where each bit in the generated stream has the same probability of being a 0 or 1 as any other bit in the stream and that the bits are not correlated; that is the bits are generated from identical independent distribution. However, the bit stream is biased. The probability of a 1 is 0.5 + 0 and the probability of a 0 is 0.5 - 0, where 0 606 0.5. A simple conditioning algorithm is as follows: Examine the bit stream as a sequence of non-overlapping pairs. Discard all 00 and 11 pairs. Replace each 01 pair with 0 and each 10 pair with 1.

a. What is the probability of occurrence of each pair in the original sequence?

answer.

00: $(0.5 - \partial)^2 = 0.25 - \partial + \partial^2$

01: $(0.5 - \partial) \times (0.5 + \partial) = 0.25 - \partial^2$

10: $(0.5 + \partial) \times (0.5 - \partial) = 0.25 - \partial^2$

11: $(0.5 + \partial)^2 = 0.25 + \partial + \partial^2$

b. What is the probability of occurrence of 0 and 1 in the modified sequence?

answer.

Because 01 and 10 have equal probability in the initial sequence, in the modified sequence, the probability of a 0 is 0.5 and the probability of a 1 is 0.5.

c. What is the expected number of input bits to produce x output bits?

answer.

The probability of any particular pair being discarded is equal to the probability that the pair is either 00 or 11, which is $0.5 + 2\partial^2$, so the expected number of input bits to produce x output bits is $x/(0.25 - \partial^2)$.

4. In a public-key system using RSA, you intercept the ciphertext C = 20 sent to a user whose public key is e = 13, n = 77 . What is the plaintext M?

answer.

We note that 77 = 7 x 11. Therefore, $\phi(n) = 60$, $d = e^{-1} \bmod \phi(n)$ gives d = 37.

Hence, $M = C^d \bmod n = 48$

5. Use the fast exponentiation algorithm of Figure 9.8 to determine 6 472 mod 3415. Show the steps involved in the computation.

answer.

472 = 1 1101 1000

I	8	7	6	5	4	3	2	1	0
b_i	1	1	1	0	1	1	0	0	0
C	1	3	7	14	29	59	118	236	476
F	6	216	3321	2006	166	1416	451	1916	3346

Answer = 3346

6. Alice and Bob use the Diffie–Hellman key exchange technique with a common prime q = 157 and a primitive root a = 5.

a. If Alice has a private key $X_A = 15$, find her public key Y_A.

answer.

$5^{15} \ mod \ 157 = 79$

b. If Bob has a private key $X_B = 27$, find his public key Y_B.

answer.

$5^{27} \ mod \ 157 = 65$

c. What is the shared secret key between Alice and Bob?

answer.

$65^{15} \ mod \ 157 = \ 79^{27} \ mod \ 157 = 78$

7. Suppose Alice and Bob use an Elgamal scheme with a common prime q = 157 and a primitive root a = 5.

a. If Bob has public key $Y_B = 1\ 0$ and Alice chose the random integer k = 3, what is the ciphertext of M = 9 ?

answer.

$10^3 \ mod \ 157 = 58$

$C_1 = 5^3 \ mod \ 157 = 125$

$C_2 = 58 \times 9 \ mod \ 157 = 51$

ciphertext $C = (125, 51)$

b. If Alice now chooses a different value of k so that the encoding of M = 9 is C = (25, C_2), what is the integer C_2 ?

answer.

$5^k \ mod \ 157 = 25$

$k = 2$

$10^2 \ mod \ 157 = 100$

$C_2 = 100 \times 9 \ mod \ 157 = 115$

8. Consider the elliptic curve $E_7(2,1)$; that is, the curve is defined by $y^2 = x^3 + 2x + 1$ with a modulus of p = 7 . Determine all of the points in $E_7(2, 1)$. Hint: Start by calculating the right-hand side of the equation for all values of x.

Answer.

x	$(x^3 + 2x + 1) \bmod 7$	square roots mod p?	y
0	$1 \bmod 7 = 1$	yes	1, 6
1	$4 \bmod 7 = 4$	yes	2, 5
2	$13 \bmod 7 = 6$	no	
3	$34 \bmod 7 = 6$	no	
4	$73 \bmod 7 = 3$	no	
5	$136 \bmod 7 = 3$	no	
6	$229 \bmod 7 = 5$	no	

9. This problem performs elliptic curve encryption/decryption using the scheme outlined in Section 10.4. The cryptosystem parameters are $E_{11}(1, 7)$ and G = (3, 2). B's private key is $n_B = 7$.

a. Find B's public key P_B.

answer.

$P_B = n_B \times G = 7 \times (3, 2) = (6, 8)$. This answer is seen in the preceding table.

b. A wishes to encrypt the message Pm = (10, 7) and chooses the random value k = 5. Determine the ciphertext C_m.

answer.

$C_m = \{kG, P_m + kP_B\} = \{5(3, 2), (10, 7) + 5(6, 8)\} = \{(4, 8), (10, 7) + (4, 8)\} = \{(4, 8), (1, 8)\}$

c. Show the calculation by which B recovers P_m from C_m.

answer.

$P_m = (1, 8) - 7(4, 8)) = (1, 8) - (4,8) = (1, 8) + (4, 3) = (10, 7)$