1. 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, the following procedure is used.

1) Choose a random 64-bit value v

2) Generate the ciphertext c = RC4(v || k) $\oplus$ 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.

m = RC4(v || k) $\oplus$ c

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

If adversary know the key Alice and Bob used wasn't changed .He/She can know the key streams RC4(v1 || k) and RC4(v2 || k) are same when v1 = v2.

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.

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?

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

2.Suppose you have an identical and independent source of bits, where bit 1 is generated with probability 0.5+p and bit 0 is generated with probability 0.5-p, where 0<p<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?

00: $(0.5 – p)^{2} = 0.25 – p + p^{2}$

01: $(0.5 – p) \times (0.5 + p) = 0.25 – p^{2}$

10: $(0.5 + p) \times (0.5 – p) = 0.25 – p^{2}$

11: $(0.5 + p) 2 = 0.25 + p + p^{2}$

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

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 in order to generate an output bit?

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

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

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

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

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

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

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

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

4. Alice and Bob use the ElGamal scheme with a common prime q = 157 and a primitive root $\alpha = 5$. Let Bob's public key be $Y_B = 10$.

A. What is the ciphertext of M=9 if Alice chooses the random integer to be k=3?

$10^{3} \bmod 157 = 58$

$C_1 = 5^{3} \bmod 157 = 125$

$C_2 = 58x9 \bmod 157 = 51$

Ciphertext C=(125,51)

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

$5^{k} \bmod 157 = 25$

k = 2

$10^{2} \bmod 157 = 100$

$C_2 = 100x9 \bmod 157 =115$

5. Consider the elliptic curve E7(2,1), where the curve is defined by $y^2 =$

$x^3 + 2x + 1$ with the modulus p=7. Determine all of the points in $E_7(2, 1)$.

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

(0,1) , (0,6) , (1,2) , (1,5)

6. This problem performs elliptic curve encryption/decryption using the scheme described in class. The cryptosystem parameters are $E_{11}(1, 7)$ and G = (3, 2). Assume that Bob's private key is n_B=7.

A. What is Bob's public key P_B?

2G =(x′,y′)=(($\frac{3x^2+a}{2y}$)^2 -2x , $\frac{3x^2+a}{2y}(x-x')$) = (10,4)

3G = (x_3,y_3)= 2G + G = (10,4)+ (3,2)

= ($\lambda^2 - x_1 - x_2$, $-y_1 + \lambda(x_1 - x_3)$)

λ =(2-4)/(3-10)= -2 x -7^{-1} = -2 x 3 = 5

∴3G=(5^2-10-3 =1 , -4+5(10-1))=(1,8)

以此類推。

4G =(5,4) , 5G=(4,8) , 6G=(7,7) , 7G=(6,8)

PB = n_B x G = 7G = (6,8)

B. Alice wants to encrypt message P_m = (10, 7) to Bob and chooses the random value k = 5. What is the ciphertext C_m?

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 of Pm from the above ciphertext C_m and private key n_B.

P_m = (1, 8) – 7(4, 8))

= (1, 8) – (4,8)

= (1, 8) + (4, 3)

= (10, 7)