Introduction to Cryptography, Fall 2021

Homework 3

Due: 1pm, 11/10/2021 (Wednesday)

Part 1: Written Problems

1. **Suppose you have an identical and independent source of bits, where bit 0 is generated with probability 0.4 andbit 1 is generated with probability 0.6.**
   A. **Design a conditioning algorithm to generate a bit string with independent bits, where 0 and 1 appear withprobability 0.5 each.**
   B. **What is the expected number of input bits in order to generate an output bit?**

   A. 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.
   Because the probability of 10 and 01 are the same (0.4*0.6=0.24), so the output bit stream has the same probability of 1 and 0.
   B. The sum of probability of 01 and 10 is 0.4*0.6*2=0.48, so the expected number of input bits to produce x output bits is x/(0.24)

2. **Write a BBS-generator program with n=23858977l and seed=7477 to generate a string of 1,000,000 bits.**
   A. **Compute the ratios of bits 0, 1. Are both of them around 50%? If not, why?**
   B. **Compute the ratios of bit pattern '00', '01', '10', and '11'. Are all of them around 25%? If not, why?**
   <u>Note</u>: 00011 is counted as two '00', one '01 and one '11'. The ratios are 50%, 25%, 0% and 25%, respectively.

   A. Yes. The number of 0 is 499695 and the number of 1 is 500305. Both of them have ratios around 50%.
   B. Yes. The number of them are as follows 00: 124043 01: 125587 10: 126022 11: 124348
   All of them have ratios around 25%.

3. **Alice and Bob use the same RSA modulus n=143. Assume that Alice's key exponents e=7 and d=103 and Bob'spublic key exponent e=13. Assume that David encrypts a message as C=60 with Bob's public key for Bob.**
   A. **Factor n, compute Bob's private key and decrypt C.**
   B. **Show that Alice can decrypt C without factoring n=143.**

   A. n = 13*11, $\emptyset(n) = 12 * 10 = 120$, 13^{-1} mod 120 = 37(Bob's private key)
   C^{37} mod 143 = 47
   B. Alice's e*d = 721 = $k\emptyset(n) + 1$ ➔ ed – 1 = 720 = $k\emptyset(n)$
   Bob's e^{-1} mod 720 = 277 , since 277≡ Bob's d (mod $\emptyset(n)$), C^{277} mod 143 = 47

4. **Alice and Bob use the Diffie–Hellman key exchange technique with a common prime q = 131 and a primitive root α = 6. If Alice chooses X_A = 15 and Bob chooses X_B = 27, what are Y_A, Y_B and the shared secret by the method?**

   $Y_A = 6^{15}$ mod 131 = 71, $Y_B = 6^{27}$ mod 131 = 104
   Key = 71^{27} mod 131 = 104^{15} mod 131 = 71

5. **Alice and Bob use the ElGamal scheme with a common prime q = 131 and a primitive root α = 6. Let Bob's publickey be Y_B = 3.**
   A. **What is the ciphertext of M=9 if Alice chooses the random integer k=4?**
   B. **If Alice uses the same k to encrypt two messages M_1 and M_2 as (12, 65) and (12, 64), what is the relationbetween M_1 and M_2?**

A. C = (6^4 mod 131, 9*3^4 mod 131) = (117, 74)

B. 3^k * M1 mod 131 =65 ➔ 3^k*M1 = 131*t_1 + 65

3^k * M2 mod 131 =64 ➔ 3^k*M2 = 131*t_2 + 65

⇨ 3^k(M1-M2) = 131(t_1 – t_2) + 1

⇨ $(3^k)^{-1}$ mod 131 = M1-M2

⇨ M1-M2 is the modular inverse of symmetric key(3^k) under mod q(131)

6. **Consider the elliptic curve $y^2 = x^3 + 3x + 1$ over Z_7. Assume that G = (3, 3) and Bob's private key is n_B = 4.**
   A. **Compute all the points over the curve.**
   B. **What is Bob's public key P_B?**
   C. **Alice wants to encrypt message P_m = (2, 1) to Bob and chooses the random value k = 3. What is theciphertext C_m?**
   D. **Decrypt the ciphertext ((5, 1), (2, 6)) using Bob's private key.**

A.

x	(x^3 + 3x + 1) mod 7	Square roots mod 7?	y
0	1 mod 7 =1	Yes	1,6
1	5 mod 7 =5	No	
2	15 mod 7 =1	Yes	1,6
3	37 mod 7 =2	Yes	3,4
4	77 mod 7 = 0	Yes	0
5	141 mod 7 =1	Yes	1,6
6	235 mod 7 =4	Yes	2,5

(0,1), (0,6), (2,1), (2,6), (3,3), (3,4), (4,0), (5,1), (5,6), (6,2), (6,5)

B. 4G = 2(2G)

2G = $((\frac{3x^2+3}{2y})^2 - 2x, \frac{3x^2+3}{2y}(x - x') - y)$ = (5, 1)

4G = 2(2G) = (6, 2) = P_B

C. C_m = (kG, P_m + kP_B) = (3(3, 3), (2, 1) + 3(6, 2))

= ((0, 1), (2, 1) + O) = ((0, 1), (2, 1))

D. Key = 4(5, 1) = (6, 5)

(2, 6) – (6, 5) = (0, 6)