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 and bit 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 with probability 0.5 each.

   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.

   00: 0.4*0.4 = 0.16

   01: 0.4*0.6 = 0.24

   10: 0.6*0.4 = 0.24

   11: 0.6*0.6 = 0.36

   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.

   B. 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 0.16 + 0.36 = 0.52, 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?

   0: 49.97%

   1: 50.03%

   B. Compute the ratios of bit pattern ‘00’, ‘01’, ‘10’, and ‘11’. Are all of them around 25%? If not, why?

   Note: 00011 is counted as two ‘00’, one ’01 and one ‘11’. The ratios are 50%, 25%, 0% and 25%, respectively.

   00: 24.86%

   01: 25.11%

   10: 25.11%

   11: 24.92%

3. Alice and Bob use the same RSA modulus n=143. Assume that Alice's key exponents e=7 and d=103 and Bob's public 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.

   $n = 11*13$, $\emptyset(n) = (11-1)(13-1) = 120$

   $d = e^{-1} \bmod \emptyset(n) = 13^{-1} \bmod 120 = 37$

   Private key: PR = {37, 143}

   Plaintext: $M = C^d \bmod n = 60^{37} \bmod 143 = 47$

   B. Show that Alice can decrypt C without factoring n=143.

   $k * \emptyset(n) = e_A * d_A - 1 = 720$

   $e_B^{-1} \bmod (k * \emptyset(n)) = 277$

   Since $277 \bmod \emptyset(n) = 37$, $C^{277} \bmod 143 = 47$

4. Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 131 and a primitive root $\alpha = 6$. 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: $6^{15} \bmod 131 = 71$

   Y_B: $6^{27} \bmod 131 = 104$

   shared secret key: $71^{27} \bmod 157 = 104^{15} \bmod 157 = 71$

5. Alice and Bob use the ElGamal scheme with a common prime q = 131 and a primitive root $\alpha = 6$. Let Bob's public key be $Y_B = 3$.

   A. What is the ciphertext of M=9 if Alice chooses the random integer k=4?

   $3^4 \bmod 131 = 81$

   $C_1 = 6^4 \bmod 131 = 117$

   $C_2 = 81 * 9 \bmod 131 = 74$

   Ciphertext C = (117, 74)

   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 relation between M_1 and M_2?

   $3^k * M_1 \bmod 131 = 65$

   $3^k * M_2 \bmod 131 = 64$

   $3^k * M_1 = 131 * t_1 + 65$

   $3^k * M_2 = 131 * t_2 + 64$

   $(3^k)^{-1} \bmod 131 = M_1 - M_2$

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.

x	$x^3 + 3x + 1 \bmod 7$	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. What is Bob's public key P_B?

$2G = (x_2, y_2) = \left(\left(\frac{3*3^2+3}{2*3}\right)^2 - 2*3,\ \left(\frac{3*3^2+3}{2*3}\right)(3 - x_2) - 3\right) = (5, 1)$

$4G = (x_4, y_4) = \left(\left(\frac{3*5^2+3}{2*1}\right)^2 - 2*10,\ \left(\frac{3*5^2+3}{2*1}\right)(5 - x_4) - 1\right) = (6, 2)$

$P_B = n_B * G = 4G = (6, 2)$

C. Alice wants to encrypt message $P_m = (2, 1)$ to Bob and chooses the random value k = 3. What is the ciphertext C_m?

$C_m = \{kG, P_m + kP_B\} = \{3(3, 3), (2,1) + 3(6, 2)\}$

$= \{(0, 1), (2, 1) + O\} = \{(0, 1), (2, 1)\}$

D. Decrypt the ciphertext ((5, 1), (2, 6)) using Bob's private key.

(2, 6) – 4(5, 1) = (2, 6) – (6, 5) = (0, 6)