Introduction to Cryptography, Spring 2021 **Due: 5/4/ 2021 (Tuesday)**

# Homework 4

Instructor: Prof. Wen-Guey Tzeng

## Part 1: Written Problems

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

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?
   B. What is the probability of occurrence of 0 and 1 in the modified sequence?
   C. What is the expected number of input bits in order to generate an output bit?

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 $Y_A$.
   B. If Bob has a private key $X_B = 27$, find his public key $Y_B$.
   C. What is the shared secret key between Alice and Bob?

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?

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. Consider the elliptic curve $E_7(2,1)$, where the curve is defined by $y^2 = x^3 + 2x + 1$ with the modulus p=7. Determine all of the points in $E_7(2, 1)$.

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 $P_B$?
   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. Show the calculation of $P_m$ from the above ciphertext $C_m$ and private key $n_B$.

# Part 2: Programming Problem

This programming problem is to practice RSA encoding and decoding using Crypto++. Please find the related library information and examples on the Internet.

I. Read in the key length in decimal, a public key (e, n) in Hex and a message in ASCII and do encryption as described in the following table. The first row is for testing and the rest is the problem. We only deal with one-block operation. You need to check whether the message length (in bits) is strictly shorter modulus n's length.

The ASCII message is treated as an integer, for example, "Hi" = "4869" (Hex) = 18537 (decimal). Since we are dealing with very long integer, please use "Integer" class for integer operations.

| Key length (bits) | Public key=(e, n) (Hex) | Message (ASCII) | Ciphertext (Hex) |
|---|---|---|---|
| 64 | (11, b14022eef719f1bb) | "Alice" | 73dc304c7bf6a0fd |
| 128 | (11, b2c8d1404ed5fc2f7ad1254bb428f0d5) | "Hello World!" | ? |
| 256 | (10001, cf625a8e47bc1cf9a3b517b31d870108c0cd97466003842a3b394d6cd857e9b7) | "RSA is public key." | ? |

II. Read in key length in decimal, private key (d, n) in Hex and a ciphertext (in Hex) and do decryption as described in the following table. The first row is for testing and the rest is the problem.

| Key length (bits) | (d, n) (Hex) | Ciphertext (Hex) | Message ( ASCII) | Public key (Hex) |
|---|---|---|---|---|
| 64 | (16282b21a7866bf5, 9d001e6473dfacf9) | 154c638cd3615216 | "Secret" | 10001 |
| 256 | (12e6a85100b889c9905a939b274a91bc57ca85d52e6c464fb455c86a29d63c89, d6361e40b2d619970ead338912a273adb75a4ce21356304834753fe94e6de24b) | a1676afd68a2fc67dac32c633600b76fa90aca9f9cca5201490a20c8b01a061a | ? | ? |

III. Submission: you need to upload two files: rsa.cpp and out.txt, where out.txt consists of 4 lines for the answers in the above problems.

IV. If you want to generate some RSA keys for practice, try the following program segment:

```
// random number generator
AutoSeededRandomPool rng;

InvertibleRSAFunction parameters;

// Generate RSA keys with key_length bits
int key_length = 256;
parameters.GenerateRandomWithKeySize(rng, key_length);

const Integer& n = parameters.GetModulus();
const Integer& p = parameters.GetPrime1();
const Integer& q = parameters.GetPrime2();
const Integer& d = parameters.GetPrivateExponent();
const Integer& e = parameters.GetPublicExponent();
```