Chiffrement et Codes Correcteurs

Nasko Karamanov

Table des matières

1 Integrer Factorization and Discret Logarithm Problem

1.1 Mathematical background

In this section we review and complete the mathematical background needed for this chapter.

Learning outcomes
— Use the algorithms of a given cryptosystem scheme
— Use an attack algorithm to decrypt cipher message.
— Estimate complexity of a given algorithm (encryption, decryption or attack)

Question 1-1 Many cryptosystems use exponential calculation in their encryption or decryption algorithms. The following algorithm often called ***square and multiply*** speeds up the process.

Let

$$e = \sum_{i=0}^{l} 2^i e_i \text{ where } e_i \in \{0,\ 1\}$$

Then

$$m^e = \prod m^{2^i e_i}$$

This already shows that it is sufficient to calculate only power of 2 exponential. For example if $l=4$ then

$$m^e = m^{2^4 e_4} \cdot m^{2^3 e_3} \cdot m^{2^2 e_2} \cdot m^{2 e_1} \cdot m^{e_0}$$

We can also obtain this product by successive multiplications. Again, if $l=4$ we have

$$\begin{array}{lllll} t_5 & = & 1 & & \\ t_4 & = & t_5^2 \cdot m^{e_4} & = & m^{e_4} \\ t_3 & = & t_4^2 \cdot m^{e_3} & = & m^{2e_4+e_3} \\ t_2 & = & t_3^2 \cdot m^{e_2} & = & m^{2^2 e_4 + 2e_3 + e_2} \\ t_1 & = & t_2^2 \cdot m^{e_1} & = & m^{2^3 e_4 + 2^2 e_3 + 2e_2 + e_1} \\ t_0 & = & t_1^2 \cdot m^{e_0} & = & m^{2^4 e_4 + 2^3 e_3 + 2^2 e_2 + 2e_1 + e_0} \end{array}$$

We notice that at each step we square and multiply. Multiplication can be skipped if the exponent is 0.

a) Determine $7^{87} \mod 34$ with square and multiply algorithm.

b) Compare the complexity of naive algorithm for m^e and the one of the square and multiply algorithm.

Training session

c) Calculate
— $9^{127} \mod 23$
— $24^{320} \mod 29$

Question 1-2
Recall that if p is a prime and $a \neq 0$ then Fermat's little theorem says

$$a^{p-1} \equiv 1 \mod p$$

This theorem can be used both to simplify exponential calculations and to calculate multiplicative inverses modulo p. Indeed $a \cdot a^{p-2} \equiv 1 \mod p$ so $a^{-1} \equiv a^{p-2} \mod p$

a) Using the remark above and square and multiply algorithm calculate $11^{187} \mod 31$

b) What is the inverse of 5 in $\mathbb{Z}/31\mathbb{Z}$?

Question 1-3 Using extended euclidean algorithm calculate the multiplicative inverse if possible of

a) $7 \in \mathbb{Z}/38\mathbb{Z}$

b) $6 \in \mathbb{Z}/28\mathbb{Z}$

Training session

c) Calculate
— u and v such that $456u + 123v = \gcd(456, 123)$
— $23^{-1} \in \mathbb{Z}/156\mathbb{Z}$
— $43^{-1} \in \mathbb{Z}/93\mathbb{Z}$

Question 1-4 The Chinese reminder theorem (CRT) gives a solution to the following congruence equations

$$\begin{array}{lll} x & \equiv & a \mod m \\ x & \equiv & b \mod n \end{array}$$

where $\gcd(m,n) = 1$ and the solution is unique modulo $N = mn$. Let u and v be such that $mu + nv = 1$. Then the solution is given by

$$x \equiv anv + bmu \mod N$$

a) Check that x is indeed a solution

b) Find the solution modulo 266 of

$$\begin{array}{lcll} x & \equiv & 4 & \mod 7 \\ x & \equiv & 9 & \mod 38 \end{array}$$

Training session

c) Solve the following system of congruence equations

$$\left\{\begin{array}{lcll} x & \equiv & 11 & \mod 23 \\ x & \equiv & 4 & \mod 156 \end{array}\right. \qquad \left\{\begin{array}{lcll} x & \equiv & 12 & \mod 43 \\ x & \equiv & 5 & \mod 93 \end{array}\right.$$

Remarks

— The CRT can be restated as the following ring isomorphism.

$$\begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \cong & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x & \longrightarrow & (x \mod m,\ x \mod n) \end{array}$$

which can be generalized for $n_1, n_2, \ldots n_k$ pairwise coprime :

$$\mathbb{Z}/n_1 n_2 \cdots n_k\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

— The solution can be writen as

$$x \equiv ann' + bmm' \mod N$$

where m' is (a lift of) the multiplicatif inverse of m modulo n and n' (a lift of) the multiplicative inverse of n modulo m.

1.2 Using cryptosystem schemes

In this section we review cryptosystems seen in the lecture course.

Learning outcomes
— Use the algorithms of a given cryptosystem scheme
— Use an attack algorithm to decrypt cipher message.
— Estimate complexity of a given algorithm (encryption, decryption or attack)

Question 1-5

a) Formalize substitution cipher scheme (seen in the video lecture) i.e. describe $(\mathscr{M}, \mathscr{C}, \mathscr{K}, \mathrm{Enc}, \mathrm{Dec})$. What is the cardinal of $\mathscr{K}$?

b) Alice and Bob agree on the secret key $\sigma = (1\ 4\ 8)(2\ 5\ 3\ 7\ 6)$. Bob received the cipher **GDBC**. What message did Alice send ? What do you think about the key ?

Training session

c) Formalize Cesar scheme (seen in the video lecture) i.e. describe $(\mathscr{M}, \mathscr{C}, \mathscr{K}, \mathrm{Enc}, \mathrm{Dec})$. What is the cardinal of $\mathscr{K}$?

Question 1-6
Alice and Bob decide to use ElGamal cryptosystem with $p = 23$ and $g = 5$.

a) Describe the set of messages and ciphered messages.

b) Bob's public key is $\mathrm{pk} = 17$. Alice wants to send the messages $\boldsymbol{m} = 13$ with her private key $a = 3$. What cipher message will Bob receive ?

c) Bob has received a second ciphertext from Alice : $\boldsymbol{c} = (21, 17)$. This ciphertext was intercepted by Eve.
   1. What is the problem Eve is confronted with ?
   2. Eve decides to use Shank's baby-step giant step algorithm to find Bob's private key. What is the key she found ?
   3. Was was the message Alice sent ?

d) Alice and Bob decide to convert letters to numbers by using their alphabet order : $A \to 01$, $B \to 02$, ... They then encrypt there message by block of two letters. What is the problem with the current cryptosystem and what should they do to correct it ?

Training session - RSA

e) Alice and Bob use RSA with $p = 7$, $q = 13$, $e = 7$ and $m = 8$. Calculate d and c.
Alice and Bob use RSA with $p = 3$, $q = 11$, $e = 7$ and $c = 8$. Calculate d and m.

1.3 Discovering a new cryptosystem

There are many cryptosystems based on integer factorization problem. One of them is Rabin's cryptosystem (1979)
Learning outcomes
— Use the algorithms of a given cryptosystem scheme
— Estimate complexity of a given algorithm (encryption, decryption or attack)
— Identify algorithms that are susceptible to be not quantum resistant
— Explain some standard techniques of perturbation/secure of standard cryptosystems.

Question 1-7 Rabin's cryptosystem with primes $p, q \equiv 3 \mod 4$
— **KeyGen**
  — Choose primes p and q such that $p \equiv q \equiv 3 \mod 4$, $n = pq$, $\mathrm{pk} = n$, $\mathrm{sk} = (p, q)$

— $\mathscr{M} = \mathscr{C} = [\![0,1]\!]$
— **Encryption**
— $\boldsymbol{c} = \mathrm{Enc}(\boldsymbol{m}, \mathrm{sk}) = m^2$
— **Decryption (computing $\sqrt{\boldsymbol{c}}$)**
— $x_1 = \boldsymbol{c}^{\frac{p+1}{4}} \mod p$ and $x_2 = \boldsymbol{c}^{\frac{q+1}{4}} \mod q$
— Use Chinese reminder theorem applied to $\pm x_1 \mod p$ and $\pm x_2 \mod q$ to find four solutions $\boldsymbol{m}_{1,2,3,4}$ modulo n.

a) Check that $x_1^2 = c \mod p$ (use Fermat's little theorem)

b) Is this cryptosystem a post-quantum one ?

c) What is the complexity of the encryption algorithm ?

d) Explain one this cryptosystem is determinstic and how to inscure semantic security.

e) Let $p = 43$ and $q = 47$. Encrypt the message $\boldsymbol{m} = 506$.

f) Alice and Bob agreed that their message should be the smallest of all four possibilities. Decrypt $\boldsymbol{c} = 59$.

1.4 Security

In this section we adress the securty of chryptosystems from diffrent point of view and we introduce the notion of digital signature.

Learning outcomes
— Use the algorithms of a given cryptosystem scheme
— Use an attack algorithm to decrypt cipher message.
— Estimate complexity of a given algorithm (encryption, decryption or attack)
— Identify algorithms that are susceptible to be not quantum resistant
— Explain some standard techniques of perturbation/secure of standard cryptosystems.

Question 1-8 Alice decides to have two public keys e_1 and e_2 when using RSA cryptosystem with $n = pq$. She chooses e_1 and e_2 to be relatively prime. Bob encrypts the same message $\boldsymbol{m}$ with both of keys and send the cipher messages $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ to Alice. Eve managed to get both cipher messages and recover the original message. Explain how is this possible.

Question 1-9 Alice and Bob communicate using ElGamal criptosystem. Eve has find a way to calculate $g^{ab} \mod p$ from $g^a \mod p$ and $g^b \mod p$.

a) Explain how Eve can decrypt the message that Alice sent !

b) What conclusion can you make from this ?

Question 1-10 Digital signature

a) Alice and Bob agreed to use RSA criptosystem. Bob received en encrypted message using his public key (n, e) ? Can he be sure it come from Alice ?

b) Alice found a solution to this problem. She encrypted her message $\boldsymbol{m}$ using Bob's public key e_B but and then sent $(\boldsymbol{c}, \boldsymbol{m}^{d_A})$ where d_A is her private key.
Can Bob now be sure that the message comes from Alice ?

c) Formalize the notion of digital signature containing three algorithms : KeyGen, Sign, Verify

d) Explicit the algorithms for Alice and Bob situation. This is called ***RSA signature***.

e) Can you think of a disadvantage of this signature and maybe a solution ?

f) What can you say about the complexity of RSA signature ?

g) Is this signature post-quantum resistant ?