Cryptography & Encryption:6G7Z1011: Lab Questions

Keith Yates

February 22, 2019

Cryptography & Encryption:6G7Z1011 : ElGamal's Encryption

1 Cryptography & Encryption:6G7Z1011 : ElGamal's Encryption

Recall, the Diffie-Hellman key exchange allowed Alice and Bob to share a secret key, it did not however achieve the goal of letting Alice and Bob securely exchange any piece of information they wished. The first algorithm that did achieve this is was the *ElGamal* public key crypto system and we discuss it now.

1.1 the ElGamal algorithm - encryption

Bob wishes to send a message securely to Alice. The usual syntax is in place: for example, $K_{A,Pr}$ is a key belonging to Alice and it is private, and $K_{A,Pu}$ is a key belonging to Alice and it is public, and p is a prime number.

1. Alice picks a prime p and g of large prime order (their values are public knowledge).
2. Alice picks a private key $K_{A,Pr}$ ($1 \leq K_{A,Pr} \leq p-1$) and publishes her public key
$$\text{Alice's public key} = K_{A,Pu} = g^{K_{A,Pr}} \mod p. \tag{1}$$
3. Bob's message M is a number between $2 \leq M < p$. He picks a number k satisfying $0 < k < p$ and now computes
$$c_1 = g^k \mod p \quad \text{and} \quad c_2 = MK_{A,Pu}^k \mod p. \tag{2}$$
4. Bob sends the numbers c_1 and c_2 to Alice.

1.1.1 ⇝: summary

In summary: if Bob wished to send the message M to Alice he sends the pair of numbers (c_1, c_2).

1.2 the same two tasks

We now face the usual two tasks:

1. Showing that Alice can convert c_1 and c_2 into M, and do so in a reasonable amount of time.
2. Showing that Eve cannot convert c_1 and c_2 into M in a reasonable amount of time.

1.3 Alice's tasks

Alice receives c_1 and c_2 and can evaluate

$$x = c_1^{K_{A,Pr}} \mod p \quad \text{and} \quad x^{-1} \mod p. \tag{3}$$

Recall eqn. 1

$$K_{A,Pu} = g^{K_{A,Pr}} \mod p. \tag{4}$$

and eqn. 2

$$c_1 = g^k \mod p \quad \text{and} \quad c_2 = MK_{A,Pu}^k \mod p. \tag{5}$$

Now note

$$\begin{aligned} x^{-1}c_2 &= (c_1^{K_{A,Pr}})^{-1}c_2 \mod p \qquad (\text{since } x = c_1^{K_{A,Pr}} \mod p) \\ &= (g^{kK_{A,Pr}})^{-1}MK_{A,Pu}^k \qquad (\text{eqn. 5}) \\ &= (g^{kK_{A,Pr}})^{-1}M(g^{K_{A,Pr}})^k \qquad (\text{eqn. 4}) \\ &= (g^{kK_{A,Pr}})^{-1}g^{kK_{A,Pr}}M \\ &= M. \end{aligned} \tag{6}$$

1.4 Eve's tasks

Note Eve has no easy way of evaluating x, because eqn. 3 contains mention of $K_{A.Pr}$. To assess the security of the algorithm we need to look at the *discrete log problem*

1.5 discrete log problem

Let G be a group and fix a $g \in G$ with order n. We seek the smallest $x \in \mathbb{N}$ (if it exists at all) such that

$$g^x = h. \tag{7}$$

1.6 properties of the gcd(a, b)

⌜ Fix two nonzero integers a and b. Then a and b have a greatest common denominator d, $d > 0$, and there exists integers α and β such that

$$d = \alpha a + \beta b. \tag{8}$$

⌟

Proof. The number 1 divides both a and b so a and b have a common positive divisor, and as the set of divisors of a and b is finite then a and b must have a greatest common denominator and being greater than or equal to 1 then it is positive. Define

$$D = \{xa + yb \mid x, y \in \mathbb{Z}\} \tag{9}$$

then D clearly contains positive elements, and we claim $d = am+bn = \min D$ is the greatest common denominator of a and b.

1. We have $a = dq + r$, where $0 \leq r < d$. Then

$$r = a - dq = a - (am + bn)q = a(1 - mq) - bnq \in D, \tag{10}$$

this contradicts the minimality of d unless $r = 0$, so $a = dq$.

2. We have $b = dq_1 + r$, where $0 \leq r < d$. Then

$$r = b - dq_1 = b - (am + bn)q_1 = b(1 - nq_1) - amq_1 \in D, \tag{11}$$

this contradicts the minimality of d unless $r = 0$, so $b = dq_1$.

1 and 2 imply $d \mid a$ and $d \mid b$, and we have established d is a common divisor of a and b. Now let c be any common divisor of a and b, that is $c \mid a$ and $c \mid b$, but $d = am + bn$ so $c \mid d$ and we deduce d is the greatest common denominator of a and b.

□

1.7 inverses

⌜ Let a, b be integers then $ab = 1 \mod m$ if and only if $\gcd(a, m) = 1$ ⌟

Proof. $\Rightarrow$: Let $\gcd(a, m) = 1$ then §1.6 implies $1 = \alpha a + \beta m$. That is

$$\alpha a - 1 = -\beta m \quad \text{thus} \quad \alpha a = 1 \mod m. \tag{12}$$

$\Leftarrow$: Let $ab = 1 \mod m$ then $ab - 1 = cm$ and thus $\gcd(a, m)$ divides $ab - cm = 1$, so $\gcd(a, m) = 1$.
□

2 Problems & Supplementary Material:Problems

2.1 problem:

⌜Write Java code that implements the ElGamal public key encryption algorithm. In the notation of the slides.

1. Suppose Alice takes the prime p to be 467 and let $g = 2$, what is the value of her public key $K_{A,Pu}$?
2. Bob wishes to send the message $M = 331$. He picks $k = 197$. What are the values c_1 and c_2 he generates? (recall this is the ciphertext sent to Alice)
3. Alice computes $x = c_1^{K_{A,Pr}}$ and thus x^{-1} and finally $c_2 x^{-1}$; thus there are three steps — we can perform all three in a reasonable amount of time.

⌟

2.2 problem:Shank's little step - big step algorithm

⌜Code the Shank's little step - big step algorithm. ⌟

2.3 problem:Shank's little step - big step algorithm

⌜Using Shank's algorithm solve

$$g^x = h \tag{13}$$

in $\mathbb{F}_p^*$ with $g = 9704$, $h = 13896$ and $p = 17389$.
⌟

2.4 problem:

⌜Write a Java function that solves the Chinese remainder theorem when there are two equations.
⌟

2.5 problem:

⌜Let G be a group of order 4. Prove that either G is cyclic, or every element of G is its own inverse. Deduce any group of size 4 is Abelian. ⌟

2.6 problem:

⌜Continue with assignment. ⌟