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

Keith Yates

February 22, 2019

# Plan of Lecture

Plan:

1. We discuss the ElGamal algorithm, it is an important encryption technique, you will code it in the lecture - and I will provide a solution.
2. The lecture is technical - I have provided a crib sheet.

# ElGamal

The ElGamal encryption algorithm (ElGamal 1985) is an asymmetric key encryption algorithm for public-key cryptography which is based on the DiffieHellman key exchange. We descibe it now; it involves non-trivial mathematics and non-trivial computing.

# ElGamal Public Key Encryption

We carry on from the Diffie-Hellman algorithm and discuss ElGamal's Public Key Encryption. Suppose Bob wishes to communicate securely with Alice.

1. Alice picks a prime $p$ and $g$ of large prime order (their values are public knowledge).
2. Alice picks a private key $K_{A,Pr}$ and publishes her public key

$$\text{Alice's public key} = K_{A,Pu} = g^{K_{A,Pr}} \mod p. \tag{0.1}$$

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

$$c_1 = g^k \mod p \quad \text{and} \quad c_2 = MK_{A,Pu}^k \mod p. \tag{0.2}$$

4. Bob sends the numbers $c_1$ and $c_2$ to Alice.

# Decrypting ElGamal

We have two remaining tasks:

1. Showing Alice can decrypt the message in a reasonable amount of time
2. Showing Eve has a very difficult task decrypting the message in a reasonable amount of time

# What Alice Does to Decrypt

Alice has received $c_1$ and $c_2$. Recall

$$c_1 = g^k \mod p \quad \text{and} \quad c_2 = MK_{A,Pu}^k \mod p. \tag{0.3}$$

She can evaluate both $x = c_1^{K_{A,Pr}}$ and $x^{-1}$ (in a reasonable amount of time) and then

$$\begin{aligned}
x &= c_1^{K_{A,Pr}} \\
x^{-1} &= (c_1^{K_{A,Pr}})^{-1} \\
x^{-1}c_2 &= (c_1^{K_{A,Pr}})^{-1} MK_{A,Pu}^k \\
x^{-1}c_2 &= (g^{kK_{A,Pr}})^{-1} MK_{A,Pu}^k \\
x^{-1}c_2 &= (g^{kK_{A,Pr}})^{-1} M(g^{K_{A,Pr}})^k \quad , K_{A,Pu} = g^{K_{A,Pr}} \\
x^{-1}c_2 &= (g^{kK_{A,Pr}})^{-1} Mg^{kK_{A,Pr}} \quad , \\
&= M.
\end{aligned} \tag{0.4}$$

# Work load

Equation 0.4 is correct — however we need to check all the operations can be performed in a reasonable amount of time. Eve's problem is

$$x = c_1^{K_{A,Pr}}, \tag{0.5}$$

Eve knows $c_1$ (it was sent on the insecure channel), but has no knowledge of $K_{A,Pr}$..

# A student query

Show (by direct calculation) that

$$\left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right), \left( \begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right), \left( \begin{array}{cc} -1 & 0 \\ 0 & 1 \end{array} \right), \left( \begin{array}{cc} -1 & 0 \\ 0 & -1 \end{array} \right) \tag{0.6}$$

are a group. How would you do this in Java code?

# Discrete Log Problem

Let $G$ denote a group and let $g \in G$ with order $N$, for a $h \in G$ we seek the smallest $x \in \mathbb{N}$ such that

$$g^x = h. \tag{0.7}$$

There exists an algorithm that finds $x$ in $\sqrt{N} \log n$ time, we present a simple variant.

# Shanks Little Step - Big Step Algorithm

We are given $g$ and $h$ and know $N$.

1. Let $n = 1 + \sqrt{N}$.
2. Create two lists:
   a) $1\ ,\ g,\ g^2,\ \ldots g^n$
   b) $h\ ,\ hg^{-n},\ hg^{-2n},\ \ldots hg^{-n^2}$
3. There exists a match between the two lists; that is $g^i = hg^{-jn}$.
4. $x = i + jn$ is a solution to $g^x = h$.

# Shanks Little Step- Big Step Proof

⌜A match occurs in the lists: $1$ , $g$, $g^2$, $\ldots g^n$ and $h$ , $hg^{-n}$, $hg^{-2n}$, $\ldots$. $hg^{-n^2}$. That is $g^i = hg^{-jn}$ ⌟

## Proof.

Recall we are looking for a solution to $g^x = h$. Decompose $x$

$$x = nq + r \quad \text{with} \quad 0 \leq r < n. \tag{0.8}$$

As the order of $g = N$ then $1 \leq x < N$ so

$$q = \frac{x-r}{n} < \frac{N}{n} < n \quad (\text{recall } n > \sqrt{N}.) \tag{0.9}$$

Thus $g^x = h$ may be written

$$g^r = hq^{-qn} \quad \text{with } 0 \leq q < n \quad \text{and } 0 \leq r < n. \tag{0.10}$$

# Solving Equations

We need to study more carefully the solutions sets to equations mod $n$. Recall from school

1. simple equations: $2x = 5$.
2. simultaneous equations $2x + 3y = 1$ , $x + 7y = 4$.
3. quadratic equations $x^2 + 3x + 1 = 0$.
4. simultaneous quadratic equations $x^2 + 3xy + y^2 = 0$. $2x^2 + xy + 3y^2 = 0$.

And so on:

# The natural questions

Given a collection of equations, natural equations arise: does it have have solutions? And if so, how many solutions does the equation have?
The answers (of course) depend on the values in the equations.

# very simple example

1. $y = x^2 + 1$ then $x^2 + 1 = 0$ has no solutions.
2. $y = x^2$ then $x^2 = 0$ has one solution
3. $y = x^2 - 1$ then $x^2 - 1 = 0$ has two solutions.

On the real line, a polynomial of order $n$ has between 0 and $n$ solutions; it can not have more than $n$ solutions.
If the above is not obvious, can we draw the three graphs stated above please.

# mod $n$

The situation is more difficult in mod $n$, even very simple examples require scrutiny. Consider the equation

$$2x = 1 \mod 6. \tag{0.11}$$

and note

| x | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 2x | 0 | 2 | 4 | 0 | 2 | 4 |

Table: Calculation in mod 6.

So, there is no solution to eqn. 0.11, and NO you can not just divide by 2.

# Equations with two unknowns

The situation becomes even more difficult if we have multiple variables, and this time the problem is nothing to do with mod $n$. The equation

$$4x + 2y = 5 \tag{0.12}$$

has no integer solutions (can you see why?)

# A Little Revision

This is discussed in the notes, we have meet it briefly before but we need to go through it again. The goals are to find necessary and sufficient conditions for a range of equations to have solutions.

# 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 $\alpha$ and $\beta$ such that

$$d = \alpha a + \beta b. \tag{0.13}$$

⌟

# proof 1

## 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

$$D = \{xa + yb \mid x, y \in \mathbb{Z}\} \tag{0.14}$$

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

# proof 2

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

$$r = a - dq = a - (am + bn)q = a(1 - mq) - bnq \in D, \tag{0.15}$$

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

$$r = b - dq_1 = b - (am + bn)q_1 = b(1 - nq_1) - amq_1 \in D, \tag{0.16}$$

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 $b$

# 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 $1 = \alpha a + \beta m$. That is

$$\alpha a - 1 = -\beta m \quad \text{thus} \quad \alpha a = 1 \mod m. \tag{0.17}$$

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

# Simultaneous Equations

We raise the stakes, consider

$$x = a \mod m \quad \text{and} \quad x = b \mod n \tag{0.18}$$

Can we find a $x$ such that both equations are satisfied simultaneously? (In general no.)

# Chinese Remainder Theorem

The Chinese mathematician Sun-Tsu asked the following question

- Find a number that leaves a remainder of 1 when divided by 3, a remainder of 2 when divided by 5, and a remainder of 3 when divided by 7 .

The question appears in Master Suns Mathematical Manual, written between 287 A.D. and 473 A .D:

# In Modern Terminology

We wish to solve simultaneously the following equations.

$$x = 1 \mod 3, \quad x = 2 \mod 5, \quad \text{and } x = 3 \mod 7. \tag{0.19}$$

Have a go.

# Answer 1

We have $x = 1 + 3t_1$ $(t_1 \in \mathbb{Z})$ substitute in $x = 2 \mod 5$

$$\begin{aligned} 1 + 3t_1 &= 2 \mod 5 \\ 3t_1 &= 1 \mod 5 \\ t_1 &= 2 \mod 5 \end{aligned} \tag{0.20}$$

That is $t_1 = 2 + 5t_2$ $(t_2 \in \mathbb{Z})$

# Answer 2

We have $t_1 = 2 + 5t_2$ $(t_1 \in \mathbb{Z})$ substitute in $x = 2 \mod 5$

$$\begin{aligned} x = 1 + 3t_1 &= 1 + 3(2 + 5t_2) \\ x &= 7 + 15t_2 \end{aligned} \tag{0.21}$$

Finally as $x = 3 \mod 7$ we deduce

$$\begin{aligned} 7 + 15t_2 &= 3 \mod 7 \\ 15t_2 &= 3 \mod 7 \\ t_2 &= 3 \mod 7 \end{aligned} \tag{0.22}$$

so $t_2 = 3 + t7$ $(t \in \mathbb{Z})$ and (nearly there)

$$\begin{aligned} x = 7 + 15t_2 &= 7 + 15(3 + t7) \\ x &= 52 + 105t \end{aligned} \tag{0.23}$$

# The Chinese Remainder Theorem

The linear system of congruences

$$x = a_i \mod m_i \tag{0.24}$$

where the $\{m_i \mid 1 \leq i \leq n\}$ are relatively prime has a unique solution mod $m_1 m_2 \ldots m_n$.