Public Key Cryptography

Lecture 7

The ElGamal Public Key Cryptosystem and Finite Fields

Index

The ElGamal Public Key Cryptosystem

- ElGamal (1985)
- Based on the following problems, solvable only by exponential-time algorithms:

Discrete Logarithm Problem (DLP)

Let $(G, \cdot)$ be a finite cyclic group with n elements, having a generator g and let $y \in G$. Determine a power x $(0 \leq x \leq n-1)$ such that $y = g^x$ (we formally write $x = log_g y$).

Diffie-Hellman Problem (DHP)

Let $(G, \cdot)$ be a finite cyclic group with n elements, having a generator g and let $g^a, g^b \in G$ for some $a, b \in \{0, \ldots, n-1\}$. Determine g^{ab}.

Conjecture

DLP and DHP are computationally equivalent.

The ElGamal cryptosystem (basic version)

1. Key generation. Alice creates a public key and a private key.

1.1. Generates a large random prime p and a generator g of $(\mathbb{Z}_p^*, \cdot)$.
1.2. Selects a random integer a $(1 \leq a \leq p-2)$.
1.3. Computes $g^a \bmod p$.
1.4. Alice's public key is (p, g, g^a); her private key is a.

2. Encryption. Bob sends an encrypted message to Alice.

2.1. Gets Alice's public key (p, g, g^a).
2.2. Represents the message as a number m between 0 and $p-1$.
2.3. Selects a random integer k $(1 \leq k \leq p-2)$.
2.4. Computes $\alpha = g^k \bmod p$ and $\beta = m \cdot (g^a)^k \bmod p$.
2.5. Sends the ciphertext $c = (\alpha, \beta)$ to Alice.

3. Decryption. Alice decrypts the message from Bob.

3.1. Uses the private key a to get the message $m = \alpha^{-a}\beta \bmod p$.

The ElGamal cryptosystem (generalized version)

1. Key generation. Alice creates a public key and a private key.

1.1. Selects an appropriate cyclic group $(G, \cdot)$ of order n with a generator g.
1.2. Selects a random integer a $(1 \leq a \leq n - 1)$.
1.3. Computes g^a in the group G.
1.4. Alice's public key is (g, g^a) together with a description of how to multiply elements in G; her private key is a.

2. Encryption. Bob sends an encrypted message to Alice.

2.1. Gets Alice's public key (g, g^a).
2.2. Represents the message as an element m of the group G.
2.3. Selects a random integer k $(1 \leq k \leq n - 1)$.
2.4. Computes $\alpha = g^k$ and $\beta = m \cdot (g^a)^k$ in the group G.
2.5. Sends the ciphertext $c = (\alpha, \beta)$ to Alice.

The ElGamal cryptosystem (generalized version) (cont.)

3. Decryption. Alice decrypts the message from Bob.

3.1. Uses the private key a to get the message $m = \alpha^{-a}\beta$ in the group G.

Theorem

The ElGamal algorithm is correct.

Proof. We have $\alpha^{-a} \cdot \beta = g^{-ak} m \cdot (g^a)^k = m$.

Remarks.

- The difficulty of the Discrete Logarithm Problem (Diffie-Hellman Problem) does not depend on the generator.
- Interesting for cryptography:
  $G = F_q^*$ for some finite field F_q with q elements ($q = p^m$ and p prime).
- GNU Privacy Guard, PGP

The ElGamal Cryptosystem - example

Example.

- *Key generation.*
  Alice selects the prime $p = 2357$ and a generator $g = 2$ of the group $(\mathbb{Z}^*_{2357}, \cdot)$.
  Then she chooses $a = 1751 \leq p - 2$ and computes
  $g^a \bmod p = 2^{1751} \bmod 2357 = 1185$.
  Alice's private key is 1751; her public key is $(2357, 2, 1185)$.
- *Encryption.*
  To encrypt the message $m = 2035$, Bob selects a random
  $k = 1520 \leq p - 2$ and computes
  $\alpha = g^k \bmod p = 2^{1520} \bmod 2357 = 1430$ and
  $\beta = m \cdot (g^a)^k \bmod p = 2035 \cdot 1185^{1520} \bmod 2357 = 697$.
  Then he sends the message $(\alpha, \beta) = (1430, 697)$ to Alice.
- *Decryption.*
  To decrypt, Alice computes $m = \alpha^{-a}\beta \bmod p =$
  $\alpha^{p-1-a}\beta \bmod p = 1430^{605} \cdot 697 \bmod 2357 = 2035$.

Polynomials

- $K[X]$ denotes the ring of polynomials over a field K.
- The rings $\mathbb{Z}$ and $K[X]$ have some similar properties.

Definition

Let $f, g \in K[X]$, $f \neq 0$, $g \neq 0$. A polynomial $d \in K[X]$ is called a *g.c.d.* of f and g (denoted (f, g)) if:
(1) $d|f$ and $d|g$;
(2) $d_1 \in K[X]$, $d_1|f$ and $d_1|g \Rightarrow d_1|d$;
(3) d is monic (that is, its leading term coefficient is 1).

Condition (3) ensures the uniqueness of g.c.d.

Polynomials (cont.)

Division Algorithm

Let $f, g \in K[X]$ with $g \neq 0$. Then $\exists! q, r \in K[X]$ such that $f = gq + r$, where $deg(r) < deg(g)$.

(f, g) is computed by the Euclidean Algorithm.

Theorem (The Extended Euclidean Algorithm)

Let $f, g \in K[X]$. If $d = (f, g)$, then $\exists u, v \in K[X]$: $d = fu + gv$. In particular,

$$(f, g) = 1 \Leftrightarrow \exists u, v \in K[X] : 1 = fu + gv \Leftrightarrow \exists f^{-1} \bmod g.$$

In this case, $f^{-1} \bmod g = u$.

Irreducibility and factorization

Definition

An $f \in K[X]$ with $deg(f) \geq 1$ is called *irreducible* if it cannot be written as $f = g \cdot h$ for $g, h \in K[X]$ with $deg(g) \geq 1$, $deg(h) \geq 1$.

Theorem (Bézout)

Let $f \in K[X]$ and $a \in K$. Then $f(a) = 0 \Leftrightarrow X - a | f$.
In particular, if $deg(f) \geq 2$ and f has a root in K, then f is reducible.

Example.

- $f \in \mathbb{C}[X]$ is irreducible $\Leftrightarrow deg(f) = 1$;
- $f \in \mathbb{R}[X]$ is irreducible $\Leftrightarrow deg(f) = 1$ or $deg(f) = 2$ with $\Delta < 0$.
- $f = X^2 + 2 \in \mathbb{Z}_3[X]$ is reducible, because $f(1) = 0$.
- $f = X^4 + 2X^2 + 1 = (X^2 + 1)^2$ is reducible in $\mathbb{Z}_3[X]$, but f has no root in $\mathbb{Z}_3$.

Irreducibility and factorization (cont.)

Theorem

Let p be a prime and $k \in \mathbb{N}^*$. Then:
(i) The product of all monic irreducible polynomials in $\mathbb{Z}_p[X]$ having the degree a divisor of k is equal to $X^{p^k} - X$.
(ii) If $f \in \mathbb{Z}_p[X]$ has degree m, then

$$f \text{ is irreducible } \Leftrightarrow (f, X^{p^i} - X) = 1, \quad \forall i \in \left\{1, \ldots, \left[\frac{m}{2}\right]\right\}.$$

Unique Factorization

$\forall f \in K[X]$ has a unique (up to the order of factors) writing $f = a \cdot f_1 \cdot f_2 \cdot \ldots \cdot f_r$, for $a \in K$, $f_1, \ldots, f_r \in K[X]$ irreducible monic.

Congruences

Definition

Set $f \in K[X]$. Define on $K[X]$ a relation:

$$g \equiv h \pmod{f} \Leftrightarrow f|g-h\,.$$

Theorem

(i) If $f \neq 0$, then $g \equiv h \pmod{f} \Leftrightarrow g, h$ give the same remainder when divided by f.
(ii) "$\equiv$" is an equivalence relation on $K[X]$ and $K[X]/$"$\equiv$" is a partition of $K[X]$.

Denote this partition by $K[X]/(f)$ and its elements by $\widehat{g}$, $\widehat{h}$ or by $g \bmod f$, $h \bmod f$ etc.

Define $\forall \widehat{g}, \widehat{h} \in K[X]/(f)$,

$$\begin{cases} \widehat{g} + \widehat{h} = \widehat{g+h} \\ \widehat{g} \cdot \widehat{h} = \widehat{g \cdot h}. \end{cases}$$

Theorem

(i) $(K[X]/(f), +, \cdot)$ *is a commutative unitary ring.*
(ii) If $deg(f) = n$, *then*

$$K[X]/(f) = \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \mid a_0, \ldots, a_{n-1} \in K\},$$

where $x = \hat{X}$. *Hence it is a vector space of dimension* n *over* K, *having the basis* $(1, x, \ldots, x^{n-1})$.
(iii) $f \in K[X]$ *is irreducible* $\Leftrightarrow$ $(K[X]/(f), +, \cdot)$ *is a field.*

Chinese Remainder Theorem

Chinese Remainder Theorem

Consider the system $\begin{cases} h \equiv g_1 \pmod{f_1} \\ \ldots\ldots\ldots \\ h \equiv g_r \pmod{f_r} \end{cases}$ where $f_1, \ldots, f_r \in K[X]$ are distinct irreducible monic polynomials and $g_1, \ldots, g_r \in K[X]$. Then the system has a unique solution modulo $f = f_1 f_2 \ldots f_r$, namely

$$h = \sum_{i=1}^{r} g_i F_i K_i,$$

where $F_i = \frac{f}{f_i}$ and $K_i = F_i^{-1} \bmod f_i$, $i = 1, \ldots, r$.

Similarities between the rings $\mathbb{Z}$ and $K[X]$

- Both of them are integral domains.
- Every integer can be represented in the form $a_0 + a_1 \cdot 10 + \cdots + a_n \cdot 10^n$, whereas every polynomial can be represented in the form $a_0 + a_1 X + \cdots + a_n X^n$.
- The Division Algorithm, the (Extended) Euclidean Algorithm, the Chinese Remainder Theorem and the Unique Factorization Theorem hold for both of them.
- By using congruences, we may construct

$$\begin{aligned} \mathbb{Z}/(n) &= \{x \bmod n \mid x \in \mathbb{Z}\} \quad (n \in \mathbb{Z}) \\ K[X]/(f) &= \{g \bmod f \mid g \in K[X]\} \quad (f \in K[X]). \end{aligned}$$

- $\mathbb{Z}/(n)$ is a field $\Leftrightarrow$ n is prime;
  $K[X]/(f)$ is a field $\Leftrightarrow$ f is irreducible.

Definition

A group $(G, \cdot)$ is called cyclic if there exists $x \in G$ such that $G =< x >$, that is, $G = \{x^k \mid k \in \mathbb{Z}\}$.
Here x is called a generator of G.

Examples.
(a) $(\mathbb{Z}, +)$ is cyclic, since $\mathbb{Z} =< 1 >$.
(b) $(\mathbb{Z}_n, +)$ is cyclic, since $\mathbb{Z}_n =< \widehat{1} >$.
(c) The group $(U_n, \cdot)$ of the n-th roots of unity is cyclic. Indeed, $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ has n elements, namely

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)^k = \varepsilon_1^k\,,$$

for $k = 0, 1, \ldots, n-1$. Then $U_n =< \varepsilon_1 >$.
A generator of U_n is called a *primitive root of unity*.

Cyclic groups (cont.)

Definition

Let $(G, \cdot)$ be a group and $x \in G$. We say that x has finite order if $\exists m \in \mathbb{N}^*$: $x^m = 1$. In this case,

$$ord\, x = min\{k \in \mathbb{N}^* \mid x^k = 1\}$$

is called the order of x.

Theorem

Let $(G, \cdot)$ be a finite cyclic group with n elements generated by an element x. Then $ord\, x = n$ and

$$G =< x >= \{1, x, x^2, \ldots, x^{n-1}\}.$$

Theorem (Lagrange)

Let $(G, \cdot)$ be a finite group. Then $\forall x \in G$, $ord\, x$ divides $|G|$.

Cyclic groups (cont.)

Theorem

Let $(G, \cdot)$ *be a cyclic group,* $G =< x >$, $|G| = n$ *and let* $k \in \mathbb{N}^*$. *Then*

$$G =< x^k > \Leftrightarrow (n, k) = 1\,.$$

Examples. (a) Consider the group $(U_8, \cdot)$ of 8-th roots of unity. Then $U_8 = \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_7\}$, where

$$\varepsilon_k = (\varepsilon_1)^k = \left(\cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}\right)^k, \quad k = 0, 1, \ldots, 7.$$

Its generators are ε_1, $\varepsilon_3 = \varepsilon_1^3$, $\varepsilon_5 = \varepsilon_1^5$ and $\varepsilon_7 = \varepsilon_1^7$. These are the primitive 8-th roots of unity.
(b) Consider the group $(\mathbb{Z}_{12}, +)$. Its generators are $\widehat{1}$, $\widehat{5}$, $\widehat{7}$, $\widehat{11}$.

Generators of a finite cyclic group

Theorem

Let $(G, \cdot)$ be a finite cyclic group with n elements. Then:
(i) There are $\varphi(n)$ (Euler's function) generators of G.
(ii) The probability of a random element of G to be a generator is $\varphi(n)/n$, which is at least $1/(6 \log\log n)$.

Generator Algorithm

- Input: a finite cyclic group G with $n = p_1^{k_1} \dots p_r^{k_r}$ elements.
- Output: a generator g of G.
- Algorithm:

  1. Choose a random element g of G.
  2. For $i = 1$ to r do

     $a := g^{\frac{n}{p_i}}$.

     If $a = 1$ then go to Step 1.
  3. Output(g).

Galois fields

Theorem (Wedderburn)

Every finite division ring is commutative.

Definition

Let $(K, +, \cdot)$ be a finite field. Then the order of 1 in the group $(K, +)$ is called the *characteristic* of K and is denoted by $char(K)$.

Example. $char(\mathbb{Z}_p) = p$ (p prime).

Theorem

Let K be a finite field. Then $char(K)$ is a prime.

Theorem

*(i) If K is a finite field, then $|K| = p^n$, with p prime and $n \in \mathbb{N}^*$.
(ii) For every prime p and every $n \in \mathbb{N}^*$, there exists a unique (up to an isomorphism) field with p^n elements.*

The unique field with p^n elements is denoted by F_{p^n} and is sometimes called the *Galois field* with p^n elements.

Example. The fields with less than 20 elements are: F_2, F_3, F_4, F_5, F_7, F_8, F_9, F_{11}, F_{13}, F_{16}, F_{17}, F_{19}.

Theorem

Let F_q be a finite field, where $q = p^n$ for some prime p. Then $char(F_q) = p$.

Galois fields (cont.)

Corollary

Let F_q be a finite field with $char(F_q) = p$. Then

$$\forall a, b \in F_q, \ (a+b)^p = a^p + b^p \, .$$

Theorem

Let F_q be a finite field. Then:
(i) $(F_q^*, \cdot)$ is a cyclic group and $\forall a \in F_q$, $a^q = a$.
(ii) If g is a generator of F_q^*, then

$$g^k \text{ is a generator of } F_q^* \Leftrightarrow (k, q-1) = 1.$$

Construction of finite fields

- If $f \in \mathbb{Z}_p[X]$ (p prime) is irreducible and $deg(f) = n$, then

  $$\mathbb{Z}_p[X]/(f) = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \mid a_0, \ldots, a_{n-1} \in \mathbb{Z}_p\}$$

  is a field with p^n elements (where $x = \hat{X}$).
- The addition and the multiplication are done modulo f and the inverse of an element is computed by the Extended Euclidean Algorithm or by using $a^q = a$, $\forall a \in F_q^*$.

Theorem

$\forall n \in \mathbb{N}^*$, $\forall p$ prime, $\exists f \in \mathbb{Z}_p[X]$ irreducible of degree n.

- Hence every finite field F_{p^n} can be seen as having the form $\mathbb{Z}_p[X]/(f)$, where $f \in \mathbb{Z}_p[X]$ is irreducible and has degree n.

Construction of finite fields - example

Example. Let us construct $F_8 = F_{2^3}$.

- Here $p = 2$ and $n = 3$, so that we need $f \in \mathbb{Z}_2[X]$ irreducible of degree 3.
- For instance, $X^3 + 1$ is reducible, because it has the root 1.

  Let us try
  $$f = X^3 + X + 1 \in \mathbb{Z}_2[X].$$
  If f were reducible, then f would be the product of a polynomial of degree 2 and a polynomial of degree 1, hence it would have a root in $\mathbb{Z}_2$. But $f(0) = 1$ and $f(1) = 1$. Hence f is irreducible.
- Now we have
  $$\begin{aligned} F_8 = \mathbb{Z}_2[X]/(f) &= \{a_2x^2 + a_1x + a_0 \mid a_0, a_1, a_2 \in \mathbb{Z}_2\} \\ &= \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}. \end{aligned} \tag{1}$$

  This is called the *polynomial representation* of the field and is very convenient for addition and subtraction.

Construction of finite fields - example (cont.)

- We can use the following facts:

  (i) Since we work modulo $f \in \mathbb{Z}_2[X]$, $x^3 + x + 1 = 0$.

  (ii) Since $char(F_8) = 2$, $a + a = 0$, $\forall a \in F_8$.

  (iii) $(F_8^*, \cdot)$ is a cyclic group.

- Let us find a generator of the cyclic group $(F_8^*, \cdot)$.

  Let us compute the powers of the first non-trivial element, namely x. In algorithms we compute $x^3 \bmod f = x + 1$, $x^4 \bmod f = x^2 + x$ etc. Here we use (i):

$$\begin{cases} x^3 = -x - 1 = x + 1 \\ x^4 = x^2 + x \\ x^5 = x^3 + x^2 = x^2 + x + 1 \\ x^6 = x^4 + x^3 = x^2 + x + x + 1 = x^2 + 1 \end{cases}$$

  Since all are different, we have $F_8^* = < x >$, hence

$$F_8 = \{0, 1, x, x^2, x^3, x^4, x^5, x^6\}. \tag{2}$$

  This form is called the *power representation* of the field and is very convenient for multiplying and dividing.

Discrete Logarithm Problem

- To determine the correspondence between the forms (1) and (2) of a finite field. In general, this is a difficult problem.
- Here we get the following table of discrete logarithms:

y	$\log_x y$
1	0
x	1
$x+1$	3
x^2	2
x^2+1	6
x^2+x	4
x^2+x+1	5

N. Koblitz, *A Course in Number Theory and Cryptography*, Springer, 1994.

R. Lidl, G. Pilz, *Applied Abstract Algebra*, Springer, 1998.

A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997. [http://www.cacr.math.uwaterloo.ca/hac]