8.2. El Gamal Cryptosystem

Secrecy is based on the discrete log problem.

El Gamal System

(i) Public: p large prime, a : PE mod p

(ii) Private key: some random secret $x \in \{2, \dots, p-1\}$

Public key: $y = a^x \mod p$

(iii) Message $m \in \{1, \dots, p-1\}$

Encryption: Choose some k (random, secret)

$k \in \{1, \dots, p-1\}$

Compute $K = y^k \mod p$

$C_1 = a^k \mod p$

$C_2 = K \cdot m \mod p$

Decryption: $C_1^x \mod p = K$

$m = K^{-1} C_2 \mod p$

(C_1, C_2) is the ciphertext.

Remarks: a) A second key k is chosen. The same plaintext can have different ciphertexts.

b) Closely related to the Diffie-Hellman key exchange.

c) ElGamal breaking is equivalent to ~~to~~ solving the DH-problem.

Thinking the Future
Zukunft denken

8.3. Generalized ElGamal Encryption

"ElGamal" works in any cyclic group where the discrete log problem is infeasible.

Appropriate groups

(i) $\mathbb{Z}_p^*$, p prime (see above)

(ii) $\mathbb{F}_{p^m}^*$, the multipl. group of $\mathbb{F}_{p^m}$, p prime, $m \in \mathbb{N}$.

(iii) Group of points on an elliptic curve.

Generalized ElGamal System

(i) Select a cyclic group G of order n with $\alpha \in G$
 (G will be written multiplicative)

(ii) Select a random integer x, $1 \leq x \leq n-1$
 Compute $y = \alpha^x$ in G.
 Public key: α, y, description of G
 Private key: x

(iii) Encryption:
 Represent message m as element of G
 Select random integer k, $1 \leq k \leq n-1$
 Compute $K = y^k$
 $C_1 = \alpha^k$, $C_2 = K \cdot m$
 (C_1, C_2) is the ciphertext.

(iv) Decryption:
 Compute $C_1^x \; (= \alpha^{kx} = y^k) = K$
 $m = (C_1^x)^{-1} C_2 = K^{-1} C_2$

<u>Example</u> $G = \mathbb{F}_{2^4}^*$

Elements are polynomials of degree ≤ 3 over $\mathbb{F}_2$.
Multiplication modulo the irr. polynomial

$$f(u) = u^4 + u + 1.$$

The elements $a_3 u^3 + a_2 u^2 + a_1 u + a_0 \in \mathbb{F}_{2^4}$ are represented by (a_3, a_2, a_1, a_0)

G has order 15, $a = (0010)$ is a generator.

u^k, $k = 1, \dots, 15$

u, u^2, u^3, $u+1$, u^2+u

u^3+u^2, u^3+u+1 (u^7), u^2+1, u^3+u, u^2+u+1

u^3+u^2+u (u^{11}), u^3+u^2+u+1, u^3+u^2+1 (u^{13}), u^3+1, 1 (u^{15})

- A chooses $x = 7$

  A's public key: $a = (0010)$, $y = a^7 = (1011)$

- Encryption by Bob:

  $m = (1100)$ $(= a^6)$

  B selects $k = 11$

  computes $K = y^{11} = a^{7 \cdot 11} = a^{15 \cdot 5 + 2}$

  $= a^{15 \cdot 5} \cdot a^2 = a^2 = (0100)$

  $C_1 = a^{11} = (1110)$

  $C_2 = K \cdot m = a^2 \cdot a^6 = a^8 = (0101)$

- Decryption by Alice

A compute $C_1^x = (0100) = a^2 = K$

$K^{-1} = a^{13} = (1101)$

$m = K^{-1} C_2 = a^{13} \cdot a^8 = a^6 = m$. ⌟

9.2. The Rabin Cryptosystem

"Same" as RSA with exponent $e = 2$.
However $\nexists d: d \cdot e \equiv 1 \pmod{\varphi(n)}$,
since $\gcd(e, \varphi(n)) = 2 \neq 1$.
Deciphering means to find a square root.
See Prop. 6.8:
$n = p \cdot q$, x nontrivial sol. of $x^2 \equiv 1 \pmod n$
$\Rightarrow \gcd(x+1, n) \in \{p, q\}$.
Equivalent? "Factoring vs. finding square roots mod n"
Computing square root mod p, p prime, is "easy".

Def. 9.1. c is called a quadratic residue mod n (QR mod n) if

$$\exists x: \quad x^2 \equiv c \pmod n$$ ⌟

(quadratischer Rest mod n)

RWTH AACHEN UNIVERSITY

Prop. 9.2. (Euler's Criterion)

Let $p > 2$ prime.

c QR mod p $\iff$ $c^{(p-1)/2} \equiv 1 \pmod{p}$. ⌟

Proof. (Ex)

Prop. 9.3. Let p prime, $p \equiv 3 \pmod{4}$, i.e. $p = 4k-1$, c QR mod p.
Then $x^2 \equiv c \pmod{p}$ has the only solutions

$x_{1,2} = \pm c^k \bmod p$. ⌟

Proof. $k = \frac{p+1}{4}$

$$x_{1,2}^2 \equiv (c^k)^2 \equiv c^{\frac{p+1}{2}} \equiv \underbrace{c^{\frac{p-1}{2}}}_{\equiv 1 \pmod{p}} \cdot c$$

$$\equiv c \pmod{p}$$

Assume $x^2 \equiv c \pmod{p}$, $y^2 \equiv c \pmod{p}$

$\Rightarrow x^2 - y^2 \equiv 0 \pmod{p} \Rightarrow p \mid (x+y)(x-y)$

$\Rightarrow p \mid (x+y)$ or $p \mid (x-y)$ $\Rightarrow x \equiv y \pmod{p}$ or $x \equiv -y \pmod{p}$.

Hence, $x_{1,2}$ are the only solutions. ∎

Remark: For $p \equiv 1 \pmod{4}$, there is no known eff. ~~alg.~~ deterministic alg. to compute squ. root mod p.
But there is a polynomial time prob. alg. ⌟

Thinking the Future
Zukunft denken

Compute square roots mod n, $n = p \cdot q$, p, q prime.

<u>Prop. 9.4.</u> Let $p \neq q$ prime, $n = p \cdot q$, c QR mod n. Compute by the ext. alg. $s, t \in \mathbb{Z}$ with

$$\underbrace{sp}_{=b} + \underbrace{tq}_{=a} = \gcd(p, q) = 1$$

Let $a = t \cdot q$, $b = sp$, further $x, y \in \mathbb{Z}$ with

$$x^2 \equiv c \pmod{p}$$

$$y^2 \equiv c \pmod{q}$$

The $f = ax + by$ is a solution of $f^2 \equiv c \pmod{n}$.

<u>Proof.</u> By definition

$$a \equiv 1 \pmod{p} \qquad b \equiv 0 \pmod{p}$$

$$a \equiv 0 \pmod{q} \qquad b \equiv 1 \pmod{q}$$

Moreover

$$(ax+by)^2 = a^2x^2 + 2abxy + b^2y^2$$

$$= \begin{cases} x^2 \equiv c & \pmod{p} \\ y^2 \equiv c & \pmod{q} \end{cases}$$

Hence, by Prop. 8.1 $(ax+by)^2 \equiv c \pmod{n}$.