8.2 The El Gamal Cryptosystem

Secrecy is based on the discrete logarithm problem

El Gamal System:

(i) Public : p : large prime number , a : PE modulo p

(ii) Private : Some random secret $t \in \{2, \dots, p-2\}$

Public Key : $y = a^t \bmod p$

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

Encryption : Choose some random secret $k \in \{2, \dots, p-2\}$

Compute $K = y^k \bmod p$

$C_1 = a^k \bmod p$, $C_2 = K \cdot m \bmod p$

Decryption : $C_1^t \bmod p \overset{(*)}{=} K$

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

(*) holds since : $C_1^t \equiv (a^k)^t \equiv (a^t)^k \equiv y^k \equiv K \pmod p$

(C_1, C_2) is the ciphertext

Remarks : - A second key k is chosen (by the sender), i.e., the same message can have different ciphertext

- Relation to Diffie-Hellman scheme : joint key $K = (a^t)^k \bmod p$
C_1 is the "public key" of the sender.
Y is the public key of the receiver.
Encryption is done by using (multiplying) with K

- Breaking El Gamal is equivalent to solving the DHP

8.3 Generalized El Gamal Encryption

El Gamal encryption works in any cyclic group G. Security is based on the intractability of the discrete logarithm problem in G.

List of groups that are appropriate:

i) Group of points on an elliptic curve (see AMC)

ii) $\mathbb{F}_{p^m}^*$, the multiplicative group of the finite field $\mathbb{F}_{p^m}$

p is prime, $m \in \mathbb{N}$

Generalized El Gamal system

(i) Select a cyclic group G of order n, with a PE a (G is written multiplicatively)

(ii) Select a random secret integer x $2 \leq x \leq n-1$

Compute: $y = a^x$ in G

Public key: a, y, ~~des~~ description of G

Private key: x

(iii) Encryption: Represent the message as $m \in G$

Select a random integer k: $2 \leq k \leq n-1$

Compute $K = y^k$

$$C_1 = a^k, \quad C_2 = K \cdot m$$

(C_1, C_2) is the ciphertext

(iv) Decryption Compute $C_1^x = K$

$$m = C_1^{-x} \cdot C_2 = K^{-1} C_2$$

Example: $G = \mathbb{F}_{2^4}^*$

Elements are polynomials of degree ≤ 3 over $\mathbb{F}_2$.
Multiplication is done modulo the irreducible 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 as the binary string $(a_3\ a_2\ a_1\ a_0)$.

G has order 15, $a = (0\,0\,1\,0)$ is a generator.

Verification that a is a generator, as $\{a^k \mid k = 1, \dots, 15\} = \mathbb{F}_{2^4}^*$

$u,\ u^2,\ u^3,\ u+1,\ u^2+u,\ \overset{(6)}{u^3+u^2},\ \overset{(7)}{u^3+u+1},\ \overset{(8)}{u^2+1},\ u^3+u$
$u^2+u+1,\ \underset{(11)}{u^3+u^2+u},\ u^3+u^2+u+1,\ \underset{(13)}{u^3+u^2+1},\ u^3+1,\ 1$

- A chooses $x = 7$

A's public key $a = (0\,0\,1\,0)$, $y = a^7 = (1\,0\,1\,1)$

- Encryption:

$m = (1\,1\,0\,0) = a^6$

B selects $k = 11$, $K = y^k = (a^7)^{11} = \underbrace{a^{15\cdot 5}}_{=1}{}^{+2} = a^2 = (0\,1\,0\,0)$

$C_1 = a^k = a^{11} = (1\,1\,1\,0)$

$C_2 = K \cdot m = a^2 \cdot a^6 = a^8 = (0\,1\,0\,1)$

$(C_1, C_2) = (a^{11}, a^8)$

- Decryption:

A computes $(C_1)^x = (a^{11})^7 = a^2 = K$

$K^{-1} = a^{15-2} = a^{13} = (1\,1\,0\,1)$

$m = K^{-1} C_2 = a^{13} \cdot a^8 = a^6 = (1\,1\,0\,0) = m$

9.2 / The Rabin cryptosystem

In principle like RSA with public key $e = 2$. However, $\nexists d : d \cdot e \equiv 1 \pmod{\varphi(n)}$, since $\gcd(e, \varphi(n)) = 2 \neq 1$

~~But~~ Deciphering means to compute square roots modulo n.
But computing square roots is no easier than factoring (see Prop 8
$n = p \cdot q$, x non-triv. sol of $x^2 \equiv 1 \pmod n \Rightarrow \gcd(x+1, n) \in \{p, q\}$
Computing square roots mod p, p prime is easy.

Def. 9.1 / c is called quadratic residue mod n (QR mod n)
if $\exists\, x : x^2 \equiv c \pmod n$

Prop 9.2 / (Euler's Criterion)
Let $p > 2$ prime. c is QR mod p $\Leftrightarrow$ $c^{(p-1)/2} \equiv 1 \pmod p$

Proof: Ex.

In general 9.2. provides no indication how to compute square roots

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

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

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

Assume $x^2 \equiv c \pmod p$ and $y^2 \equiv c \pmod p$

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

$\Rightarrow p \mid (x+y)$ 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 efficient deterministic alg to compute square roots modulo p. However, there is a polynomial time probabilistic alg.

Compute square roots modulo $n = p \cdot q$ as follows:

Prop 9.4 / Let $p \neq q$ primes, $n = p \cdot q$

Compute by the extended Euclidean algorithm $s, t \in \mathbb{Z}$ with

$$s \cdot p + t \cdot q = b + a = \gcd(p, q) = 1$$

Further $x, y \in \mathbb{Z}$ with

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

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

Then $f = a \cdot x + b y$ is a solution of $f^2 \equiv c \pmod n$

Proof: By definition

$$a \equiv 1 \pmod p \quad , \quad b \equiv 0 \pmod p$$

$$a \equiv 0 \pmod q \quad , \quad b \equiv 1 \pmod q$$

Moreover

$$f^2 = (a \cdot x + b y)^2 = a^2 x^2 + 2 a x b y + b^2 y^2 \equiv \begin{cases} x^2 \equiv c \pmod p \\ y^2 \equiv c \pmod q \end{cases}$$

Hence, by Prop 6.1 $(ax + by)^2 \equiv c \pmod n$

The proof is also immediate by the Chinese Remainder Theorem

Remark 9.5/ There are 4 solutions when deciphering, the right one must be identified from the context. To avoid this, repeat, e.g., the last 64 bits of each message. Be alarmed if none of the solutions have the repeated last bits.

Not. : ~~[illegible]~~ $m >> \sqrt{n}$, otherwise a solution is obtained by computing the square roots over the reals