$g^{p-1} \equiv 1 \bmod p$

g a PR if

$g^x \not\equiv 1 \bmod p$ for

$x < p-1$

$g^{\phi(m)} \equiv 1 \bmod m$

- $\phi(p) = p-1$
- $\phi(pq) = (p-1)(q-1)$

Order of $a \bmod m$ is

smallest pos integer s.t.

$a^x \equiv 1 \bmod m$.

$\text{ord}_m a$.

$1 \le \text{ord}_m a \le \phi(m)$

g is a PR mod p

iff $\text{ord}_p g = p-1$.

Fact: $a^r \equiv a^s \bmod m$

iff $r \equiv s \bmod \text{ord}_m(a)$.

Pf/ $a^r \equiv a^s \iff a^{r-s} \equiv 1 \bmod m$

$\iff \text{ord}_m a \mid r-s$

$a^{3k} \equiv (a^3)^k \equiv 1^k \equiv 1$

$a^5 \equiv a^3 \cdot a^2 \equiv a^2$

$a^r \equiv a^s \bmod p$

if $r \equiv s \bmod p-1$

Public Key cryptography.

Trapdoor function

a fn f easy to compute

hard to invert,

unless you have some extra

'trapdoor' information.

Public key encryption alg

- Key gen algorithm

  produces

  public key k_{pub}

  private key k_{priv}

- encryption algorithm

  $e_{k_{pub}} : \mathcal{M} \to \mathcal{C}$

- decryption alg

  $d_{k_{priv}} : \mathcal{C} \to \mathcal{M}$

El Gamal (1985)

Algorithm

1) Choose large prime p

$g \in \mathbb{Z}/p\mathbb{Z}$ s.t.

$\text{ord}_p(g)$ is a large prime.

2) Alice chooses secret a as k_{priv}

3) Alice computes

$A \equiv g^a \bmod p$

publishes $A = k_{pub}$

Bob wants to send Alice a # $2 < m < p$

- Bob generates random $k \in \mathbb{Z}/p\mathbb{Z}$ ephemeral key
- $C_1 \equiv g^k \bmod p$

  $C_2 \equiv m A^k \bmod p$
- Bob sends (C_1, C_2).

Alice computes

1) Alice computes

$x \equiv C_1^a \bmod p$

then computes $x^{-1} \bmod p$

2) $C_2 x^{-1} \equiv m \bmod p$.

Pf/

$x \equiv C_1^a \equiv (g^k)^a \equiv (g^a)^k = A^k$,

so $x^{-1} \equiv A^{-k}$

so $C_2 x^{-1} \equiv m A^k A^{-k} \equiv m \bmod p$.

$m \approx \log(p)$ bits

$(C_1, C_2) \approx 2 \log(p)$

Usually $p = 2q+1$

where q is prime

pick g s.t. $g^q \equiv 1 \bmod p$

b/c $\phi(p) = 2q$

has factors $1, 2, q, 2q$

so if $g^2 \neq 1$ then

$\text{ord} = q$.

This defeats an attack

based on Quadratic

Reciprocity.

Ex: $p = 467$, $g = 4$

Alice chooses $a = 155$

$A \equiv g^a \equiv 4^{155} \equiv 43 \bmod 467$

Alice publishes: A

Bob wants to send $m = 42$.

chooses $k = 187$. compute

$c_1 \equiv g^k \equiv 4^{187} \equiv 456 \bmod 467$.

$c_2 = m A^k \equiv 42 \cdot 43^{187} \equiv 67 \bmod 467$.

Transmits $(456, 67)$

$x \equiv c_1^a \equiv 456^{155} \equiv 413 \bmod 467$

$x^{-1} \equiv c_1^{p-1-a} \equiv 147 \bmod 467$

$m \equiv c_2 x^{-1} \equiv 67 \cdot 147 \equiv 9849 \equiv 42 \bmod 467$.

Cryptanalysis

Claim: ElGamal is at least as hard as D-H.

Imagine Eve has an ElGamal oracle.

finds plaintext from ciphertext.

Then Eve can break D-H in poly time.

Eve overhears Alice's $A \equiv g^a \bmod p$

Bob's $B \equiv g^b \bmod p$.

wants $g^{ab} \bmod p$.

Eve chooses random c_2

tells oracle: public key is A

ciphertext is (B, c_2)

oracle gives us

$$m \equiv (c_1^a)^{-1} c_2 \equiv (B^a)^{-1} c_2$$

$$\equiv (g^{ab})^{-1} c_2 \bmod p.$$

$$m^{-1} c_2 \equiv g^{ab} \bmod p$$

Complexity

Bob has 2 exponentiations
$O(\log(p))$ multiplications

Alice: 1 exponentiation
$O(\log(p))$ multiplications

The message expansion
doubles Bob's work
doubles bandwidth

So often use a
hybrid setup.
Use EG to transmit
asymmetric key.

RSA Encryption

published by Rivest, Shamir, Adleman 1978

discovered by Clifford Cocks 1973
published in 1997

Algorithm: Alice wants to send a message to Bob

Keygen

1) Bob chooses two primes p, q
   computes $N = pq$
   $M = (p-1)(q-1)$

2) choose number e s.t. $\gcd(e, M) = 1$.

3) publishes $K_{pub} = (N, e)$

4) computes $e^{-1} \bmod M$, calls that d.
   $K_{priv} (M, d)$.

Alice wants to send m, $1 \le m \le N$

1) compute $c \equiv m^e \bmod N$
   transmits that.

Bob
computes $c^d \bmod N$.
$c^d \equiv m \bmod N$.

Pf/ recall $ed \equiv 1 \bmod M$

$M = (p-1)(q-1) = \phi(N)$

$a^{ed} = a^{rM+1} \equiv (a^M)^r \cdot a \equiv 1^r \cdot a \bmod N$.

$c^d \equiv (m^e)^d = m^{ed} \equiv m' \equiv m \bmod N$.

Ex: Bob chooses $p = 73$
$q = 89$

$N = pq = 6497$

$M = 72 \cdot 88 = 6336$

Chooses $e = 83$

computes $d \equiv e^{-1} \equiv 6107 \mod 6336$

$k_{pub} = (N, e) = (6497, 83)$

$k_{priv} = (M, d) = (6336, 6107)$.

Alice wants to transmit 300

$C \equiv 300^{83} \equiv 4955 \mod 6497$

Bob computes $c^d \equiv 4955^{6107} \equiv 300 \mod 6497$.