PUBLIC-KEY CRYPTO

FACT. For all $a \in \mathbb{Z}_n^*$, we have:

(RSA) $\Longrightarrow$ $a^{\varphi(n)} \equiv 1 \bmod n$ $\quad (\varphi(n) = \#\mathbb{Z}_n^*)$

$\hookrightarrow$ $a^b \equiv a^{b \bmod \varphi(n)}$

$a^{p-1} \equiv 1 \bmod p$ $\quad (n = p \text{ a PRIME})$.

$b = q \cdot \varphi(n) + b \bmod \varphi(n) \Rightarrow a^b \equiv a^{q\varphi(n) + b \bmod \varphi(n)}$

$\equiv \underbrace{(a^{\varphi(n)})^q}_{1} \cdot a^{b \bmod \varphi(n)} \bmod n$

By Lagrange, the subgroup of powers

$a^0, a^1, a^2, \ldots$ has multiplicative order d s.t.

$$d \mid K = \varphi(n)$$

$$\Rightarrow a^{\varphi(n)} \equiv (a^d)^K \equiv 1 \mod n.$$

CYCLIC GROUPS. Groups $(G, \cdot)$ s.t. $\exists\, g \in G$

$$G = \{g^0, g^1, g^2, \ldots\} \quad \text{e.g. } \mathbb{Z}_p^*$$

$g = 3$ is a generator of $\mathbb{Z}_7^* = \{3^0, 3^1, \ldots, 3^5\}$

But 2 is not.

We need: PPT $\mathsf{GroupGen}(1^\lambda) \to (\mathbb{G}, g, q)$

$q = \#\,\mathbb{G}$

$(E.g.\ \mathbb{Z}_p^*\ ;\ q = p-1)$

To test if element is a generator, all we need is

$$p-1 = \prod_{i=1}^{t} p_i^{\alpha_i} \quad ; \quad 2^t \le p < 2^{\lambda+1}$$

$$\Rightarrow t \le \lambda$$

g NOT generator $\iff \exists\ 1 \le i \le t$ s.t.

$$g^{(p-1)/p_i} \equiv 1 \bmod p$$

The public-key revolution: DIFFIE-HELLMAN '76.

Alice $\underline{(\mathbb{G}, g, q) \leftarrow\$ \mathsf{GroupGen}(1^\lambda)}$ Bob (ALL OPERATIONS IN $\mathbb{G}$!)

$x \leftarrow\$ \mathbb{Z}_q$ — g^x → — ← g^y — $y \leftarrow\$ \mathbb{Z}_q$

$K = (g^y)^x$ $= g^{xy}$ — Eve. — $K = (g^x)^y$ $= g^{xy}$

Security ????

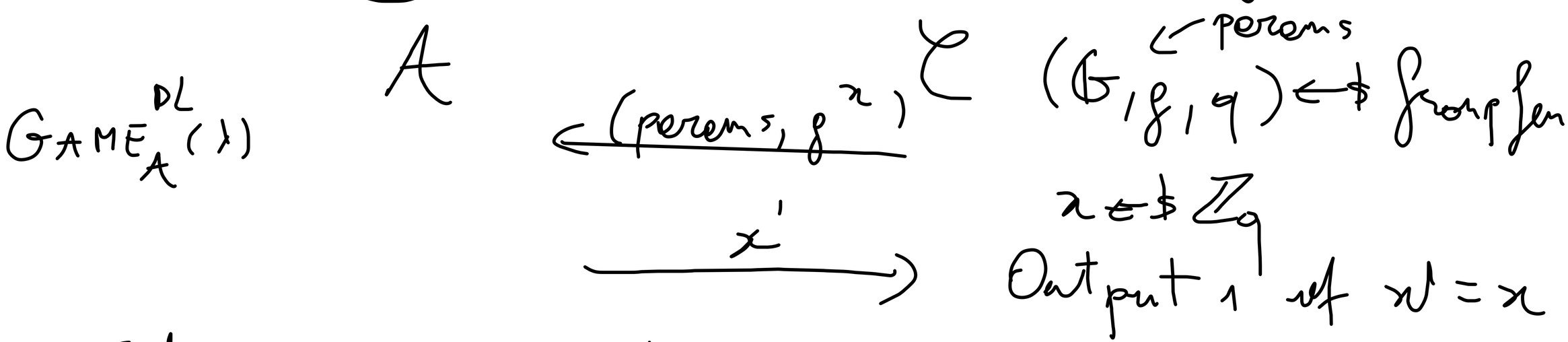
There can be many flavors. Assume EVE PASSIVE:

- If Eve can compute x (or y)

  she can compute $k = g^{xy}$

→ DISCRETE LOG

DEF The (DL) assumption holds wrt GroupGen:



$\forall$ PPT A: $\Pr[\text{GAME}_A^{DL}(\lambda) = 1] \leq \text{negl}(\lambda)$

- If we want that Eve can't compute the key $k = g^{xy}$

DEF. (CDH) The CDH ass. holds wrt groupGen:

$GAME_A^{cdh}(\lambda)$

A ⟷ C

C: $(G, g, q) \leftarrow\$ \text{groupGen}(1^\lambda)$

$C \to A$: (params, X, Y)

$x, y \leftarrow\$ \mathbb{Z}_q$; $X = g^x$; $Y = g^y$

$A \to C$: Z

Output 1 if $Z = g^{xy}$

$\forall$ PPT A: $\Pr[GAME_A^{cdh}(\lambda) = 1] \leq negl(\lambda)$

CDH $\Rightarrow$ DL. ✓

DL $\Rightarrow$ CDH ?! But nobody knows how

To solve CDH without breaking DL.

- Better definition: The key h looks random to Eve.

DEF (DDH). The DDH ass. holds wrt group fam wf:

$$(\text{params}, g^x, g^y, g^{xy}) \approx_c (\text{params}, g^x, g^y, g^z)$$

$x, y, z \leftarrow\!\!\$ \mathbb{Z}_q$; params $= (\mathbb{G}, g, q) \leftarrow\!\!\$$ GenGp

$DDH \Rightarrow CDH \ (\Rightarrow DL)$.

Bad news: $CDH / DL \not\Rightarrow DDH$. (in general)

In fact for $G = \mathbb{Z}_p^*$ DDH EASY.

Why? Consider the quadratic residues:

$$QR_p = \{ y : y = x^2 \text{ for } x \in G \}$$
$$= \{ y : y = g^z \text{ for even } z \}$$

We can test if $y \in QR_p$ by $y^{(p-1)/2} \stackrel{?}{\equiv} 1 \bmod p$

Indeed, if $y = g^{zz'}$ is a square:

$$y^{(p-1)/2} = g^{zz'(p-1)/2} = \left(g^{p-1}\right)^{z'} \equiv 1 \bmod p$$

Otherwise, $y = g^{zz'+1}$ and then:

$$y^{(p-1)/2} = g^{(zz'+1)(p-1)/2} = 1 \cdot g^{(p-1)/2} \not\equiv 1 \bmod p$$

DH-TUPLE

$\left(g^x, g^y, g^{xy}\right)$

The adversary:

- Given params, X, Y, Z
- Check if Z is square.
- If yes, $b' = 1$
  Else $b' = 0$.

$$\left| \Pr[D(\text{params}, X, Y, Z) = 1 : (X, Y, Z) \text{ is DH}] - \Pr[D(\text{params}, X, Y, Z) = 1 : (X, Y, Z) \text{ is non-DH}] \right| \geq 1/4$$

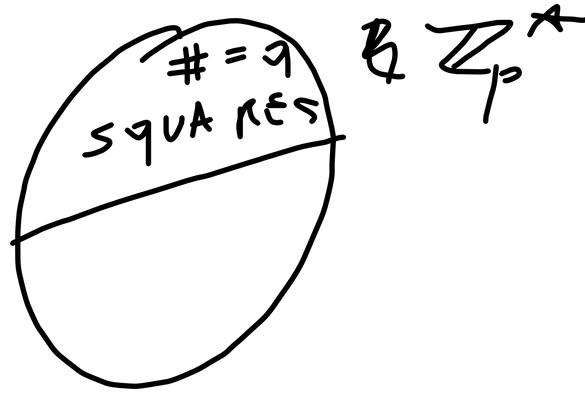
Easy way out:

- Let G be the subgroup of squares of $\mathbb{Z}_p^*$

$$\#G = q = \frac{p-1}{2} \quad ; \quad p = 2q + 1$$

- Usually p, q both primes

- Thus G is cyclic.

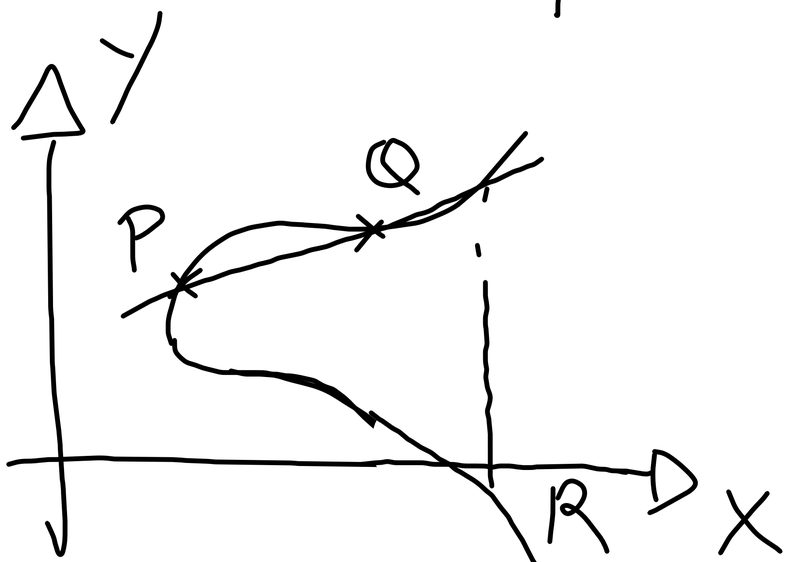


In real life: $q \approx 600$ bits; $p \approx 1024$ bits.

Here DDH believed to be HARD.

Other groups: Elliptic curves.

G: $E(\mathbb{Z}_p)$: $y = x^3 + ax^2 + bx + c \mod p$



$P + Q = R$

$E(\mathbb{Z}_p) = \{0, P, P+P, \ldots, (q-1)P\}$

$Q = xP$ x vs the DL

For us: We will mainly use FACTORING (RSA) and DDH. These assumptions are broken by QUANTUM TMs. But those don't exist yet.

↳ SHOR's ALGORITHM.

Post-quantum? (LWE), LPN, ...