Diffie-Hellman

Cyclic groups / generators / primitive roots

$\mathbb{Z}_{19}^* = \{1, \ldots, 18\}$

$\langle g \rangle = \{ g^0, g^1, g^2, \ldots \}$ (where arithmetic is mod 19)

$\langle 1 \rangle = \{1\}$

$\langle 2 \rangle = \{ 2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, \ldots \}$

$1 \quad 2 \quad 4 \quad 8 \quad 16 \quad 13 \quad 7$

$\times 2 \quad \times 2 \quad \times 2 \quad \times 2$

$2^6 \bmod 19$

$= (2^5 \bmod 19) * 2 \bmod 19$

$= \mathbb{Z}_{19}^*$

$\langle 3 \rangle = \mathbb{Z}_{19}^*$ 18 of them

$\langle 4 \rangle = \{1, 4, 16, 7, 9, 17, 11, 6, 5\}$ only 9 of them

---

Note: # of items in $\langle x \rangle$ is always divisor of $p-1$ (18 in this example)

$$\mathbb{Z}_{19}^* = \{2^0, 2^1, 2^2, 2^3, 2^4, 2^5, \ldots, 2^{17}\}$$

$$\{1, 2, 4, 8, \ldots\}$$

$$\langle 4 \rangle = \{4^0, 4^1, 4^2, 4^3, \ldots\}$$

$$= \{(2^2)^0, (2^2)^1, (2^2)^2, \ldots\}$$

$$= \{2^0, 2^2, 2^4, 2^6, 2^8, \ldots\}$$

only half of $\mathbb{Z}_{19}^*$: ones w/ even exponent when written as $\langle 2 \rangle$

---

2 is primitive root of 19

So everything in $\mathbb{Z}_{19}^*$ can be written as power of 2 (mod 19)

So every $x \in \mathbb{Z}_{19}^*$ can be written as

$$x \equiv 2^a \bmod 19$$

Define $a = \text{dlog}_2(x)$

discrete log of x (wrt base 2)

$\langle 2 \rangle = \{ 2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, \dots \}$

$1 \quad 2 \quad 4 \quad 8 \quad 16 \quad 13 \quad 7$

$\times 2 \quad \times 2 \quad \times 2 \quad \times 2$

$d\log_2(13) = 5$ because $2^5 \equiv 13$

Discrete log problem is hard for large numbers

---

we use cyclic generally only when n prime

$\mathbb{Z}_n^* = \{1, .. n-1\}$

but other n's have primitive root:

e.g. $n = 34$ $\{g, g^2, g^3, \dots\} = \mathbb{Z}_{34}^*$

Diffie-Hellman:

public: p, g s.t. $\langle g \rangle = \mathbb{Z}_p^*$

Alice		Bob
$a \leftarrow \mathbb{Z}_{p-1}$		$b \leftarrow \mathbb{Z}_{p-1}$
$A = g^a$	$\xrightarrow{A}$	
	$\xleftarrow{B}$	$B = g^b$

$K = B^a = (g^b)^a$ (shared key $= g^{ab}$) $K = A^b = (g^a)^b$

Obs: A, B public (as is p, g)

computing a from this info
is equivalent to solving discrete log

$\Rightarrow$ If eavesdropper can solve DLOG of A,
he/she knows as much as Alice did
$\Rightarrow$ can also compute K

Security: given public transcript, key K looks random

$\Updownarrow$

given $g^a, g^b \ldots g^{ab}$ looks random

Decisional Diffie-Hellman
property / assumption