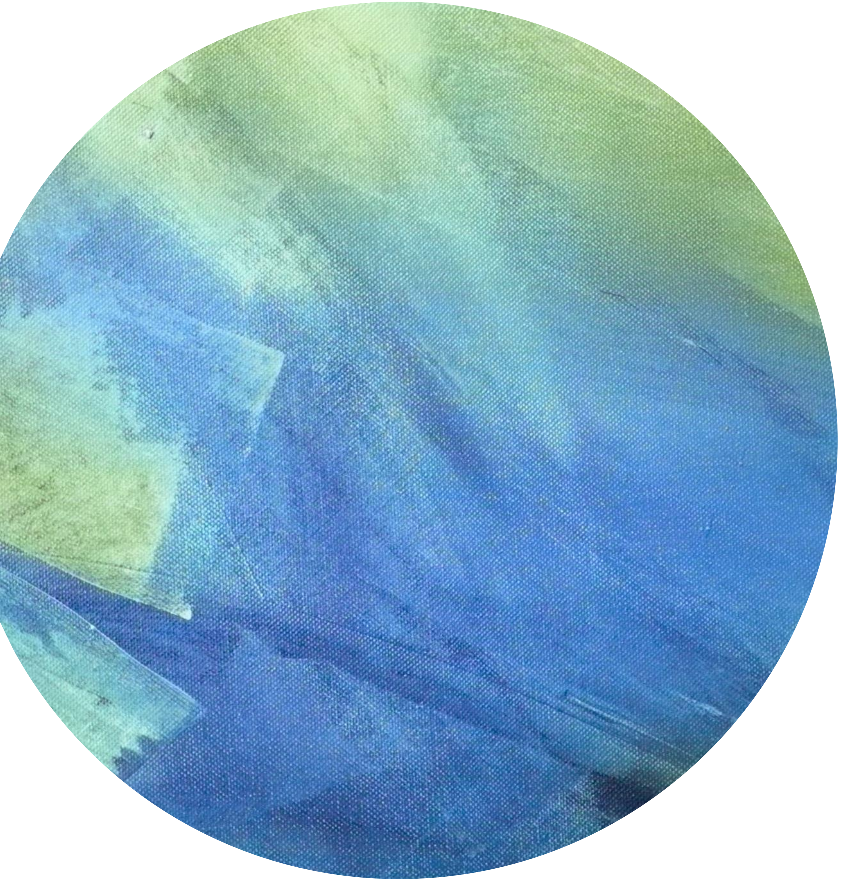
Lecture 11

Scribe: Colten



Outline

Number Theory

Key exchange

Number Theory

Number theory: Recall

N denotes an n-bit positive integer. p denotes a prime.

- Z_N = $\{ 0, 1, \ldots, N-1 \}$

- $(Z_N)^*$ = (set of invertible elements in Z_N) = $\{ x \in Z_N : \gcd(x,N) = 1 \}$ $\Longleftrightarrow$

x is invertible in Z_N if $\exists$ y in Z_N s.t. $xy = 1$ in Z_N

Can find inverses efficiently using Euclid algorithm: time = $O(n^2)$

Fermat's theorem (1640)

Thm: Let p be a prime

$$\forall x \in (Z_p)^* : \quad x^{p-1} = 1 \text{ in } Z_p$$

$\mathbb{Z}_p^* = \{1, 2, 3, 4, \dots p-1\}$

Example: p=5. $3^4 = 81 = 1$ in Z_5

$\forall x \in \mathbb{Z}_p^* : \; x^{p-1} = 1$

$\underline{x \cdot x^{p-2}} = 1$

So: $x \in (Z_p)^* \;\Rightarrow\; x \cdot x^{p-2} = 1 \;\Rightarrow\; x^{-1} = x^{p-2}$ in Z_p

$x^{p-2} = x^{-1}$

another way to compute inverses, but less efficient than Euclid

Application: generating random primes

Suppose we want to generate a large random prime

say, prime p of length 1024 bits (i.e. $p \approx 2^{1024}$)

Step 1: choose a random integer $p \in [\ 2^{1024}\ ,\ 2^{1025}-1\ ]$

Step 2: test if $2^{p-1} = 1$ in Z_p

If so, output p and stop. If not, goto step 1 .

Simple algorithm (not the best). **Pr[p not prime] < 2^{-60}**

The structure of $(Z_p)^*$ = for prime p $\{1, 2 \ldots p-1\}$. $Z_p^* = Z_p \setminus \{0\}$

<u>Thm</u> (Euler): $(Z_p)^*$ is a **cyclic group**, that is

$$\exists\, g \in (Z_p)^* \text{ such that } \{1, g, g^2, g^3, \ldots, g^{p-2}\} = (Z_p)^*$$

g is called a **<u>generator</u>** of $(Z_p)^*$

$\{1 = g^0, g = g^1, g^2, g^3, \ldots, g^{p-2}\} = Z_p^*$.

Example: p=7. $\{1, 3, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = (Z_7)^*$

Not every element is a generator: $\{1, 2, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4\}$

1 2 4 1 2 4

How do you find a generator?

Order

For $g \in (Z_p)^*$ the set $\{1, g, g^2, g^3, \dots\}$ is called
the **group generated by g**, denoted <g>

$<g>$

$<3> = Z_7^*$

$<2> = \{1, 2, 4\}$.

Def: the **order** of $g \in (Z_p)^*$ is the size of <g>

$$\mathbf{ord_p(g) = |<g>| = (\text{smallest } a>0 \text{ s.t. } g^a = 1 \text{ in } Z_p)}$$

Examples: $\underline{ord_7(3) = 6 \; ; \; ord_7(2) = 3 \; ; \; ord_7(1) = 1}$

Thm (Lagrange): $\forall g \in (Z_p)^*$: $\mathbf{ord_p(g)}$ divides p-1

$p-1 = (a_1 a_2)$

$\forall g \in Z_p^*$, $ord(g) = 1$ or a_1 or a_2 or $a_1 a_2$.

If g is gen, order $= (p-1)$.

To find generator, pick a random element and compute its order. Hit and trial works in practice as long as (p-1) is chosen wisely

Euler's generalization of Fermat (1736)

$x^{p-1} = 1$ in Z_p^*

Def: For an integer N define $\varphi(N) = |(Z_N)^*|$ (Euler's φ func.)

Examples: $\varphi(12) = |\{1,5,7,11\}| = 4$; $\varphi(p) = p-1$

For $N=p\cdot q$: $\varphi(N) = N-p-q+1 = (p-1)(q-1)$

$\varphi(N) = |Z_N^*|$

Thm (Euler): $\forall\, x \in (Z_N)^*$: $x^{\varphi(N)} = 1$ in Z_N

If $N =$ prime p, $\varphi(N) = p-1$, recover Fermat's theorem

Example: $5^{\varphi(12)} = 5^4 = 625 = 1$ in Z_{12}

Generalization of Fermat. Basis of the RSA cryptosystem

Hard Problems

Easy problems

- Given composite N and x in Z_N find x^{-1} in Z_N

- Given prime p and polynomial $f(x)$ in $Z_p[x]$

  find x in Z_p s.t. $f(x) = 0$ in Z_p (if one exists)

  Running time is linear in deg(f) .

… but many problems are difficult

Logarithm $\log_2(n) = ?$ x s.t. $2^x = n$.

Intractable problems with primes

$g^x = y$

generator .

$Z_p^* = \{1, \dots, p-1\}$.

Fix a prime p>2 and g in $(Z_p)^*$ of order q.

Consider the function: $x \longmapsto g^x$ in Z_p^*

Now, consider the inverse function:

given g, y find x s.t. $g^x = y$.

$\mathbf{Dlog_g(g^x) = x}$ **where x in {0, …, q-2}**

DISCRETE LOGARITHM

Example:

in $\mathbb{Z}_{11}^*$:	$\{$ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 $\}$
$\mathrm{Dlog}_2(\cdot)$:	

Intractable problems with primes

$p = \underbrace{\overset{n}{1024}\text{-bit}}_{\text{primes}}$

Fix a prime p>2 and g in $(Z_p)^*$ of order q.

Consider the function: $x \longmapsto g^x$ in Z_p

$Z_p^* = \{1, 2, 3 \ldots\ldots p-1\}$

$= \{1, 2, 3, \ldots\ldots 2^{128}\}.$

Now, consider the inverse function:

$\mathrm{Dlog}_g(g^x) = x$ **where x in {0, …, q-2}**

$\mathrm{Dlog}_2(y) = x$ s.t. $2^x = y$.

Example:

in $\mathbb{Z}_{11}$:	1,	2,	3,	4,	$\boxed{5,}$	6,	7,	8,	9,	10
$\mathrm{Dlog}_2(\cdot)$:	0,	1,	8,	2,	4,	9,	7,	3,	6,	5

$2^2 \neq 5$ $2^3 = 8 \neq 5$ $2^4 = 16 = 5$

DLOG: more generally

Let **G** be a finite cyclic group Z_p^* and **g** a generator of G

$$G = \{1, g, g^2, g^3, \ldots, g^{q-1}\}$$ (q is called the order of G)

Def: We say that **DLOG is hard in G** if for all efficient alg. A:

$$\Pr_{g \leftarrow G,\, x \leftarrow Z_q}\left[\, A(G, q, g, g^x) = x \,\right] \leq \text{negligible}$$

Example : $\boxed{(Z_p)^* \text{ for large } p}$

$g \quad g^2 \quad g^4 \quad g^8 \ldots$

$x = 1011$ as bitstring

$1 \quad 1 \quad 0 \quad 1$

$g^8 \cdot g^2 \cdot g$

This is a candidate **ONE-WAY FUNCTION (OWF)**
Easy to compute g^x but hard to find x given g^x

An application: collision resistance

$= Z_p^*$ $\quad$ 7 $\quad$ $H : (g, h)$ $\quad$ 3 $\quad$ 2

Choose a group G where Dlog is hard (e.g. $(Z_p)^*$ for large p)

~~Let q = |G| be a prime.~~ Choose generator g of G and set h = g^s for secret s.

Hash key = (g, h). For $x,y \in \{1,\ldots,\cancel{q}\}$ $p-1$ define $H(x,y) = g^x \cdot h^y$ in G

(x_0, y_0) (x_1, y_1) where $(x_0, x_1) \le p-1$. $(y_0, y_1) \le p-1$.

Lemma: finding collision for H(.,.) is as hard as computing $\mathrm{Dlog}_g(h)$

Proof: Suppose we are given a collision $H(x_0,y_0) = H(x_1,y_1)$ $\quad (x_0, y_0) \neq (x_1, y_1)$

then $\underbrace{g^{x_0} \cdot h^{y_0}}_{g^{x_1} h^{y_0}} = \underbrace{g^{x_1} \cdot h^{y_1}}_{g^{x_1} h^{y_0}} \Rightarrow \boxed{g^{x_0 - x_1} = h^{y_1 - y_0}} \Rightarrow h = \boxed{g^{x_0 - x_1 / y_1 - y_0}}$

g^s

$s = \left(\frac{x_0 - x_1}{y_1 - y_0}\right)$

Breaks DLOG - hardness.

If $y_0 = y_1$, $x_0 \neq x_1$ $g^{x_0} = g^{x_1}$ cannot be true for $(x_0, x_1) \leq p-1$.

$x_0 = 1$ $x_1 = p$

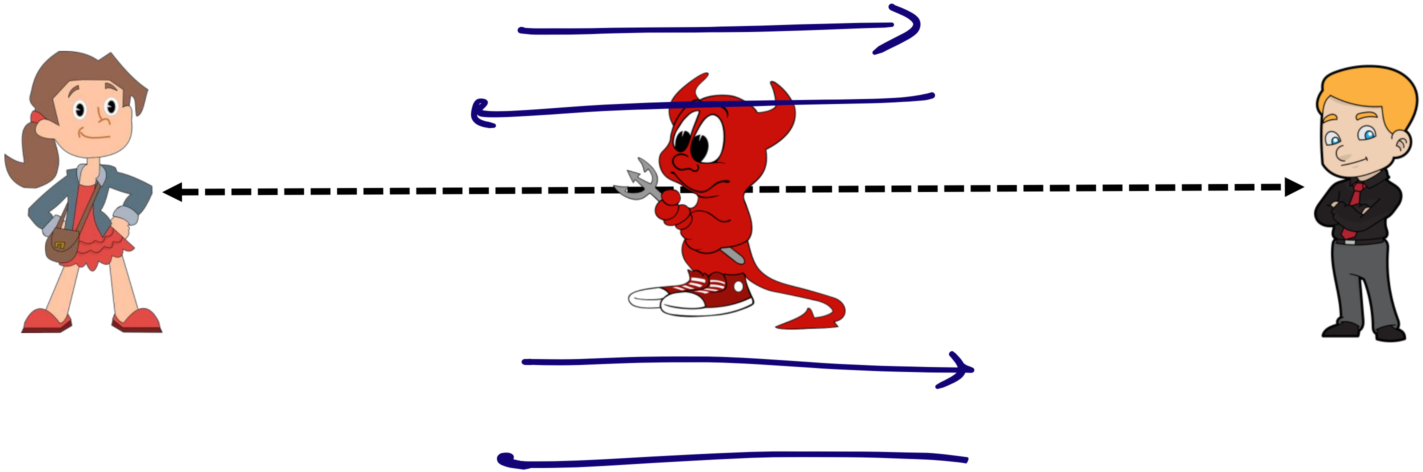
$y_0 = 1$ $y_1 = p$

Key Exchange

$H(x_0 y_0) = g^{x_0} h^{y_0} = g \cdot h$

$H(x_1 y_1) = g^{x_1} h^{y_1} = g^p h^p = g \cdot \underbrace{g^{p-1}}_{1} \cdot h \cdot \underbrace{h^{p-1}}_{1} = g \cdot h.$

Setting up a shared key in the presence of an eavesdropper



Space for Discussions - OWF + addnl properties?

$$\longleftarrow \mathbb{Z}_p^*,\ g \longrightarrow$$

a

g^a

$$\xrightarrow{g^a}$$

$$\xleftarrow{g^b}$$

b

$K = (g^b)^a = g^{ab}$

$K = (g^a)^b = g^{ab}.$

computational Diffie-Helman assumption : given g^a, g^b hard to compute g^{ab}

decisional Diffie-Helman assumption : $(g^a, g^b, g^{ab}) \approx_c (g^a, g^b, g^c)$

$a, b, c \leftarrow$ random in $\{1, .. \, p-2\}$

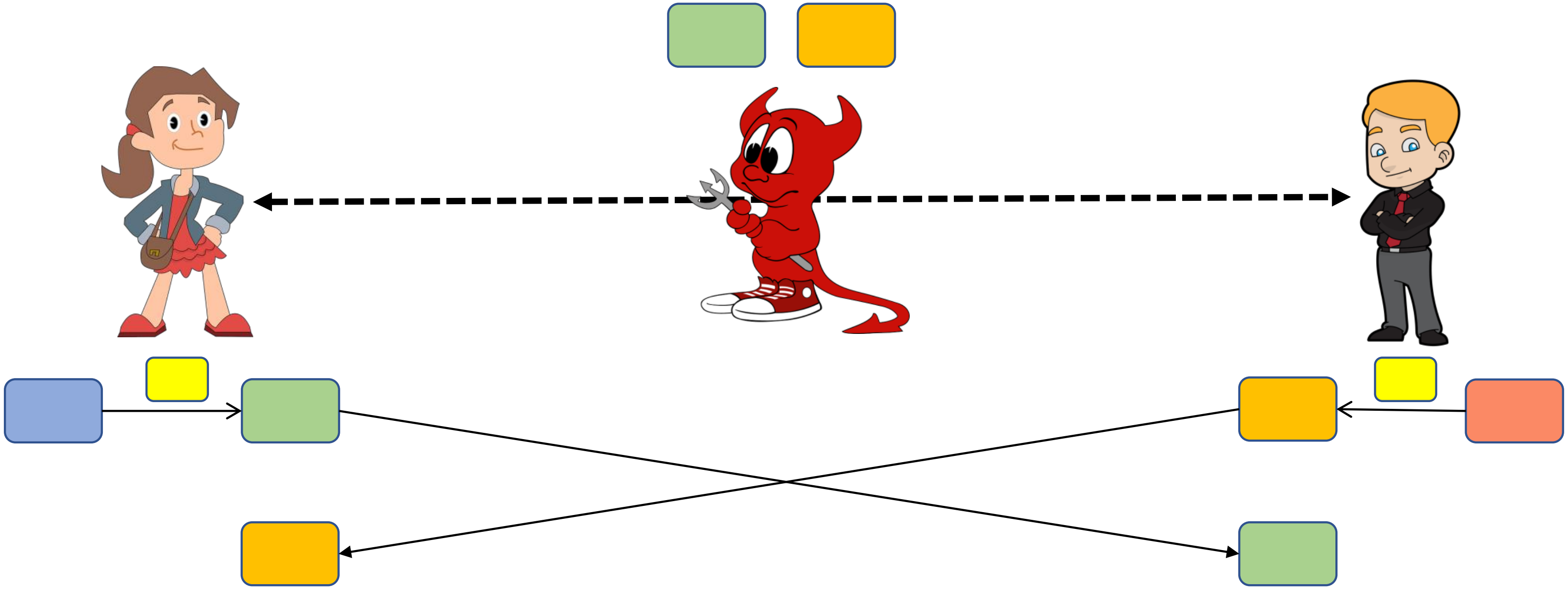
DLOG

Discrete log : given g^x, hard to find x.

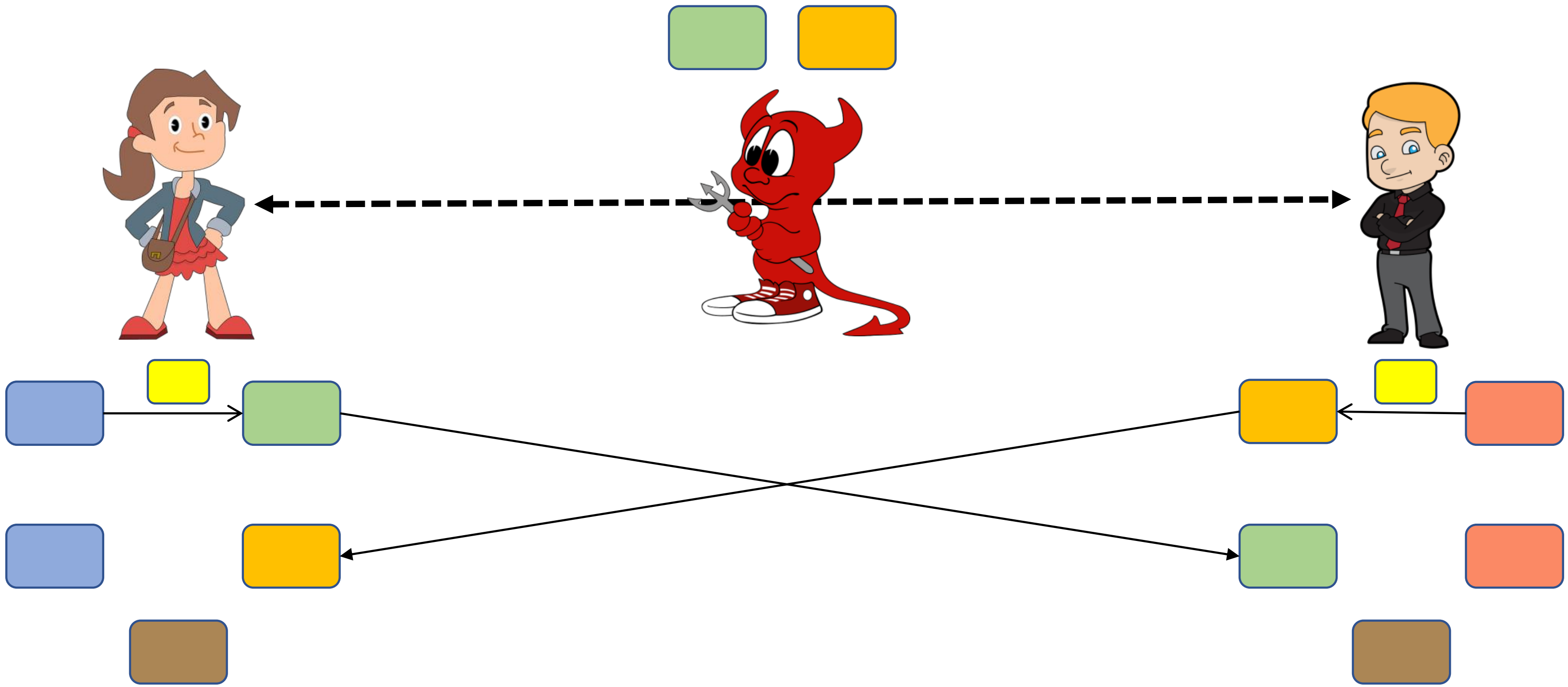
Break DLOG $\overset{\not\Leftarrow}{\Longrightarrow}$ BREAK CDH, DDH

Break CDH $\Rightarrow$ Break DDH

Setting up a shared key in the presence of an eavesdropper



Setting up a shared key in the presence of an eavesdropper



The Diffie-Hellman protocol (informally)

Fix a large prime p (e.g. 600 digits)

Fix an integer g in {1, …, p-1}

Alice **Bob**

choose random **a** in {1,…,p-1} choose random **b** in {1,…,p-1}

"Alice", $A \leftarrow g^a \pmod p$ →

← "Bob", $B \leftarrow g^b \pmod p$

$\mathbf{B^a} \pmod p = (g^b)^a = \mathbf{k_{AB} = g^{ab}} \pmod p = (g^a)^b = \mathbf{A^b} \pmod p$

Security (much more on this later)

Eavesdropper sees: p, g, $A=g^a \pmod p$, and $B=g^b \pmod p$

Can she compute $g^{ab} \pmod p$??

More generally: define $DH_g(g^a, g^b) = g^{ab} \pmod p$

How hard is the DH function mod p?

If DH is hard then DLOG is hard. If DLOG is hard then DH may or may not be hard. Both believed to be hard in Z_p^*.

Insecure against man-in-the-middle

As described, the protocol is insecure against **active** attacks