Cryptography

Encryption modes

	ECB	CBC	CTR	OFB
secure?	x	y	y	y
encryption parallel?		x	y	x
decryption parallel?		y	y	x
random access decryption?		y	y	x

Length expansion

if dec. error then
return ERROR

if dec. OK then
return $* - *$

Storage encryption

- where to store the IV or nonce?
- because expansion not possible:
  Enc $B^{512} \to B^{512}$
- $\to$ use nonce derived from address
  ESSIV: where IV for sector i is
  $IV := Enc(H(k), i)$
  encrypted salt sector IV

9 Diffie-Hellman Key Agreement

Modular arithmetic

- Integer divisions: For $a, d \in \mathbb{Z}$ there exist a unique quotient q and a unique remainder r s.t.:

$$a = d \cdot q + r \qquad\qquad and \;\; 0 \leq r \leq \mid d - 1 \mid$$

- Since q and r are unique:

$$\begin{aligned} q &= a \; \underline{div} \; d & &= \lfloor \frac{a}{d} \rfloor \\ r &= a \; \underline{mod} \; d & &= a\%d \end{aligned}$$

- Relation "divides": $a \mid d$

Congruence relation

$a \equiv b \pmod{m}$ or $a \equiv_m b$ if $m \mid (a-b)$ **"Integers mod m"**: $\mathbb{Z}_m \overset{def.}{=} \{0, 1, ..., m-1\}$
Note: $\underbrace{a \equiv_m b}_{equivalence\ relation} \neq (\underbrace{a \; mod \; m \; = \; b \; mod \; m}_{euquality\ over\ \mathbb{Z}})$
Rules: $(a + b) \; mod \; m \; = \; (((a \; mod \; m) + (b \; mod \; m)) \; mod \; m)$

Cyclic groups

Definition

A group $\langle F, \cdot, 1 \rangle$ consists of a set G, an operation $\cdot$, and a neutral element 1

1. $\forall a, b \in G : (a \cdot b) \in G$
2. $\forall a : 1 \cdot a = a \cdot 1 = a$
3. $\forall a \in G, \exists a^{-1} \in G : a \cdot a^{-1} = 1$
4. associative

Example

1. $\mathbb{Z}_m \stackrel{def}{=} \langle \mathbb{Z}_m, +, 0 \rangle$
2. $\mathbb{Z}_p^\star \stackrel{def}{=} \langle \{1, 2, ..., p-1\}, \cdot, 1 \rangle$

Definition

$\mid G \mid$ denotes the number of elements in G

Definition

A finite group G is <u>cyclic</u> if some g called <u>generator</u> exists s.t. $G = \{g^0, g^1, g^2, ...g^{|G|-1}\}$
<u>Notation</u>: $\langle g \rangle = G$
<u>Integers mod m:</u> $\langle g \rangle_m \subset \mathbb{Z}_m^\star$

Definition

If $\langle g \rangle_p = \mathbb{Z}_p^\star$, then g is a <u>primitive root</u>.

Example

$\mathbb{Z}_{11}^\star$
$\langle 1 \rangle_{11} = \{1\}$
$\langle 2 \rangle_{11} = \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\}$
$\langle 2 \rangle_{11} = \{1, 3, 9, 5, 4\}$

Definition

- The number of elements in G is also called the <u>order</u> of G
- The order of $a \in G$ is the smallest i s.t. $a^i = 1$ (in G)
  [smallest i s.t. $g^i \equiv_m 1$]

Lemma

For all primitive roots g:

$$g^a = g^b \Leftrightarrow a \equiv_{|G|} b$$

Example

- $\mathbb{Z}_p^\star,\ p\ prime : \mid \mathbb{Z}_p^\star \mid = p - 1$
- For $q \mid (p-1)$, and q prime, there is a cyclic group of order q (q prime!), defined by multiplication modulo p
  (think of: $\underbrace{p}_{safe\ prime} = 2 \cdot \underbrace{q}_{Sophie-Germain\ prime} +1$
  $p\ =\ m \cdot q + 1$, where $\mid p \mid =\ 2000$, but $q\ \approx\ 256$

Discrete Logarithms

Definition

In a cyclic group G, the discrete logarithm of $y \in G$ w.r.t a primitive root g is $x \in \mathbb{Z}_{|G|}$ s.t. $g^x = y$.

Definition

Discrete Logarithm Problem (DLP):
Given $y \leftarrow G$, compute x s.t. $g^x = y$

Group where the DLP is computationally hard:

- Prime-order subgroups of $\mathbb{Z}_p^\star$, p prime (DSA, DH)
- groups defined over points on alliptic curves (ECDSA...) $[| G | \geq 2^{256}]$

Diffie-Hellman Key Agreement

Goal

Agree on a pseudorandom key.

$$
\begin{array}{lcl}
 & G = \langle g \rangle & \\
\underline{\text{Alice}} & \text{order } q & \underline{\text{Bob}} \\
a \leftarrow \mathbb{Z}_q & & b \leftarrow \mathbb{Z}_q \\
X := g^a & \xrightarrow{x} & Y := g^b \\
Z_A := Y^a & \xleftarrow{y} & Z_B := X^b \\
 & \text{Eve} &
\end{array}
$$

<u>Claim:</u> $Z_A = Z_B$: $Z_Y = Y^a = (g^b)^a = (g^a)^b = X^b = Z_B$

Security?

- If Eve can compute DLOG, then not secure
- Want that Z is pseudorandom

Definition

Protocol Π generates a key k in $\Pi.K$ and a transcript $T \in \{0,1\}^\star$.
$(T,k) \ \leftarrow \ EXEC(\Pi)$
$K.A$ protocol Π is called secure if:

$$
\begin{array}{l}
\underline{L^{\Pi}_{ka-real}} \\
\underline{\text{Query}():} \\
\quad (T,k) \ \leftarrow \ EXEC(\Pi) \\
\quad \textbf{return } (\text{T,k})
\end{array}
\quad \approx \quad
\begin{array}{l}
\underline{L^{\Pi}_{ka-rand}} \\
\underline{\text{Query}():} \\
\quad (T,k) \ \leftarrow \ EXEC(\Pi) \\
\quad k^\star \leftarrow \Pi.K \\
\quad \textbf{return } (\text{T},k^\star)
\end{array}
$$