Notes from CS 6260 (Applied Cryptography)
Georgia Tech, Fall 2012

Christopher Martin
chris.martin@gatech.edu

1 Symmetric cryptography scheme

Key space	$\mathcal{K}$
Message space	$\mathcal{M}$
Cypher space	$\mathcal{C}$
Key generator	$\mathsf{Gen} : \phi \to \mathcal{K}$
Encryption function	$\mathsf{Enc} : \{\mathcal{K} \times \mathcal{M}\} \to \mathcal{C}$
Decryption function	$\mathsf{Dec} : \{\mathcal{K} \times \mathcal{C}\} \to \mathcal{M}$

2 Information theoretic security

Information theoretic security repels even resource-unbounded attackers. Shannon secrecy and perfect secrecy are equivalent definitions of information theoretic security for symmetric cryptography schemes.

Shannon secrecy A scheme is Shannon-secret with respect to the distribution D over $\mathcal{M}$ iff the ciphertext reveals no additional information about the message.

$$\forall\, M \in \mathcal{M},\, C \in \mathcal{C} : \Pr_{\substack{k \leftarrow \mathsf{Gen} \\ m \in D}} \big[\, m = M \,|\, \mathsf{Enc}_k(m) = C \,\big] = \Pr_{m \in D} \big[\, m = M \,\big]$$

Perfect secrecy A scheme is perfectly secret iff the distributions of ciphertexts for any two messages are identical.

$$\forall\, M_1, M_2 \in \mathcal{M},\, C \in \mathcal{C} : \Pr_{K_1 \leftarrow \mathsf{Gen}} \big[\, \mathsf{Enc}_{K_1}(M_1) = C \,\big] = \Pr_{K_2 \leftarrow \mathsf{Gen}} \big[\, \mathsf{Enc}_{K_2}(M_2) = C \,\big]$$

This model considers only a single message and ciphertext, so although a one-time pad is perfectly secret, a “two-time pad” is not.

Theorem 1. Perfect secrecy ⇒ $|\mathcal{K}| \geq |\mathcal{M}|$.

Proof. If not, $\exists$ 2 messages with different probabilities of encrypting to the same cypertext. □

3 Pseudo-random functions

Uniformly random function U is a random variable chosen uniformly from the set of all functions $\{0,1\}^m \to \{0,1\}^n$.

Pseudo-random function A PRF belongs to a family of functions $F : \{0,1\}^\ell \times \{0,1\}^m \to \{0,1\}^n$. Write $F_k(\cdot)$ to denote $F(k,\cdot)$.

Distinguishing advantage Consider an adversary $\mathcal{A}$ who knows F, having oracle access to F_k where k was chosen uniformly at random, trying to distinguish the oracle's responses from a random function. The distinguishing advantange of $\mathcal{A}$ against F is

$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \equiv \Pr_{k\in\{0,1\}^\ell}\left[\mathcal{A}^{F_k} \text{ accepts}\right] - \Pr_U\left[\mathcal{A}^U \text{ accepts}\right] .$$

In time $O(t)$, we can brute-force t keys to get advantage $t/2^\ell$.

(t,q)-bounded adversary

t	Running time
q	Number of queries

(t,q,ε)-secure PRF F is (t,q,ε)-secure iff $\forall$ (t,q)-bounded $\mathcal{A}$,

$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \varepsilon .$$

Examples of reasonable constants

t	2^{128}
q	2^{64} or 2^{32}
ε	2^{-128}

Existence The existence of secure PRFs has not been proven, but there are some functions that have never been broken and are widely assumed to be PRFs.

4 Reduction

Karp (many-to-one) reduction Reduction from A to B transforms an instance of A to an instance of B.

Cook (Turing) reduction Reduction from A to B solves A using a subroutine that solves B.

Key recovery security F is (t, q, ε)-kr-secure iff $\forall$ (t, q)-bounded $\mathcal{A}$,

$$\mathrm{Adv}_F^{\mathrm{kr}} \equiv \Pr_{k \in \{0,1\}^\ell} \left[\mathcal{A}^{F_k(\cdot)} \text{ outputs } k \right] \leq \varepsilon \ .$$

Theorem 2. If F is a (t, q, ε)-secure PRF for $q < 2^m$, then F is (t', q', ε')-kr-secure for $t' \approx t$, $q' = q - 1$, $\varepsilon' = \epsilon + 2^{-n}$.

Proof. Cook reduction. For any kr-adversary $\mathcal{A}'$ running in time t' and making $q' < 2^m$ queries, let $\mathcal{A}$ be the PRF adversary:

```
$k' \leftarrow \mathcal{A}'(\mathcal{O})$
$x \leftarrow$ a value that $\mathcal{A}'$ did not query with
$y \leftarrow \mathcal{O}(x)$
Accept iff $y = F_{k'}(x)$
```

$\mathcal{A}$ runs in time $t \approx t'$ and makes $q = q' + 1$ queries.

$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \geq \mathrm{Adv}_F^{\mathrm{kr}}(\mathcal{A}') - 2^{-n} \ . \qquad \square$$

Example PRF construction For PRF $F : \{\texttt{0},\texttt{1}\}^\ell \times \{\texttt{0},\texttt{1}\}^n \to \{\texttt{0},\texttt{1}\}^n$, $F'_k(x) \equiv F_k(F_k(x)) \| F_k(\overline{F_k(x)})$

Theorem 3. F' is $(t, \dfrac{q}{3}, \varepsilon + \dfrac{q^2}{2^n})$-secure.

Proof. Let $\mathcal{A}'$ be an attacker on F'. Define $\mathcal{A}$ as:

```
$\mathcal{O}' \equiv \mathcal{O}(\mathcal{O}(x)) \| \mathcal{O}(\overline{\mathcal{O}(x)})$ (done with 3 queries to $\mathcal{O}$)
Accept iff ${\mathcal{A}'}^{\mathcal{O}'}$ accepts
```

$\mathcal{O}'(x)$ simulates F' perfectly, so $\Pr_k \left[\mathcal{A}^{F_k} \right] = \Pr_k \left[{\mathcal{A}'}^{F'_k} \right]$.

$\mathcal{O}'$ does not simulate U perfectly, but it is close. We have independence as long as all of the $\mathcal{O}(x)$, $\overline{\mathcal{O}(x)}$ are distinct. Using union bound, this probability $\leq \frac{q^2}{2^n}$ $\square$

5 Pseudo-random permutations

In a permutation family $F : \{0,1\}^\ell \times \{0,1\}^n \to \{0,1\}^n$, every F_k is bijective.

A secure PRP is computationally indistinguishable from a uniformly random permutation.

Some well-known PRPs	DES	$\ell = 56$	$n = 64$
	AES_{128}	$\ell = 128$	$n = 128$
	AES_{192}	$\ell = 192$	$n = 128$

Strong PRP / block cipher Attackers with oracle access to both F and F^{-1} have small advantage.

$$\mathrm{Adv}_F^{\mathrm{sprp}} \equiv \Pr_k \left[\mathcal{A}^{F_k, F_k^{-1}} \text{ accepts} \right] - \Pr_P \left[\mathcal{A}^{P, P^{-1}} \text{ accepts} \right] \le \varepsilon$$

PRF/PRP switching lemma If G is a (t, q, ε)-secure PRP (not necessarily strong), then F is a $(t, q, \varepsilon + \frac{q^2}{2^{n+1}})$-secure PRF.

6 Secure symmetric encryption

Perfect secrecy is impossible where $m > \ell$, but computational security is possible with pseudorandom objects.

Electronic code block (ECB) Suppose F is a secure PRP $\{\mathtt{0},\mathtt{1}\}^\ell \times \{\mathtt{0},\mathtt{1}\}^n \to \{\mathtt{0},\mathtt{1}\}^n$ with F and F^{-1} efficiently computable.

Gen	$k \leftarrow \{\mathtt{0},\mathtt{1}\}^\ell$
Enc	$M' \leftarrow$ Pad message M with `1` and some `0`s to a multiple of n. Break M' into n-bit blocks $m_0, m_1, \ldots$ Apply F_k to each of the $\{m\}$
Dec	Apply F_k' to each of the $\{m\}$

Repeated blocks give repeated ciphertext. Never use ECB.

Security model Adversary, seeing all cipthertexts and having oracle access to Enc_k, learns nothing about plaintexts (except message length, which is unavoidable).

$SE = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is (t, σ, ε)-IND-CPA secure ("indistinguishable under chosen-plaintext attack") iff $\forall$ (t, σ)-bounded $\mathcal{A}$,

$$\mathrm{Adv}^{\mathrm{indcpa}}_{SE}(\mathcal{A}) \equiv \Pr_{k \leftarrow \mathsf{Gen}}\left[\mathcal{A}^{L_k} \text{ accepts}\right] - \Pr_{k \leftarrow \mathsf{Gen}}\left[\mathcal{A}^{R_k} \text{ accepts}\right] ,$$

$$L_k(m, m') \equiv \mathsf{Enc}_k(m) \text{ if } |m| = |m'| \text{ else } \perp ,$$

$$R_k(m, m') \equiv \mathsf{Enc}_k(m') \text{ if } |m| = |m'| \text{ else } \perp ,$$

t is the running time, and σ total length of all message queries.

Equivalent definition: Enc_k is computationally indistinguishable from a zero-encrypting oracle $Z_k \equiv \mathsf{Enc}_k(\mathsf{0}^m)$.

Query repetition Enc in an IND-CPA-secure scheme should not always return the same ciphertext for multiple encryptions of the same message. This attack has advantage 1 against any deterministic and stateless scheme:

```
$c \leftarrow \mathcal{O}(\langle 0 \rangle, \langle 0 \rangle)$
$c' \leftarrow \mathcal{O}(\langle 0 \rangle, \langle 1 \rangle)$
Accept iff $c = c'$
```

7 Block cipher modes

Stateful counter mode (CTRS) Let F be a PRF with $m = n$.

```
Gen   $k \leftarrow \{0,1\}^\ell$, $counter \leftarrow 0$
Enc   echo $counter$
      for each message block $m$:
          echo $F_k(counter) \oplus m_i$
          increment $counter$
```

CTRS is not used much, because preserving *counter* is difficult.

Theorem 4. If F is a (t, q, ε)-secure PRF, then CTRS(F) is $(t' \approx t, qn, 2\varepsilon)$-IND-CPA secure.

Proof. We will show using a hybrid argument that $\forall$ (t', σ)-bounded $\mathcal{A}'$ against CTRS(F) where $\sigma \leq n\,2^m$, there is a $(t \approx t', q = \sigma/n)$-bounded attacker $\mathcal{A}$ attacking F such that $\mathrm{Adv}^{\mathrm{indcpa}}_{\mathrm{CTRS}(F)}(\mathcal{A}') \leq 2\,\mathrm{Adv}^{\mathrm{prf}}_{F}(\mathcal{A})$.

Given $\mathcal{O}$ that is either F or U:

```
$\mathcal{A} \equiv \mathcal{A}_L \equiv$
    $\textit{counter} \leftarrow 0$
    $\mathcal{O}'(m, m') \equiv$
        If $|m| = |m'|$, return $\bot$
        Split $m$ into blocks $m_0, m_1, \ldots, m_{t-1}$
        $y_i \leftarrow \mathcal{O}(\textit{counter} + i)\ \forall\ i \in [0, t)$
        Return $\textit{counter} \| \mathrm{join}_i(m_i \oplus y_i)$
        $\textit{counter} \leftarrow \textit{counter} + t$
    Accept iff ${\mathcal{A}'}^{\mathcal{O}'}$ accepts
```

Also define $\mathcal{A}_R$ similarly using m' instead of m.

$\mathcal{A}_L^{F_k}$ perfectly simulates L_k to $\mathcal{A}'$.

$\mathcal{A}_L^{U}$ does not simulate R_k, but it does simulate an oracle \$:

```
$\$(m, m') \equiv$
    If $|m| = |m'|$, return $\bot$
    Return $\textit{counter} \|$[random bits]
    $\textit{counter} \leftarrow \textit{counter} +$ number of blocks
```

$$\begin{aligned}
P_\ell &= \Pr_k[\mathcal{A}_L^{F_k}] = \Pr_k[{\mathcal{A}'}^{L_k}] \\
P_r &= \Pr_k[\mathcal{A}_R^{F_k}] = \Pr_k[{\mathcal{A}'}^{R_k}] \\
P_\$ &= \Pr_k[\mathcal{A}_L^{U}] = \Pr_k[\mathcal{A}_R^{U}] = \Pr_k[{\mathcal{A}'}^{\$}]
\end{aligned}$$

$$\begin{aligned}
\mathrm{Adv}^{\mathrm{indcpa}}_{\mathrm{CTRS}(F)}(\mathcal{A}') &= |P_\ell - P_r| \\
&\le |(P_\ell - P_\$) + (P_r - P_\$)| \qquad \text{(triangle inequality)} \\
&\le \varepsilon + \varepsilon = 2\varepsilon
\end{aligned}$$

□

Counter modes

CTRS	One global counter	$\mathrm{adv}^{\mathrm{indcpa}} \le 2\,\mathrm{adv}^{\mathrm{prf}}$
CTR\$	Random IV for each message	$\mathrm{adv}^{\mathrm{indcpa}} \le 2\,\mathrm{adv}^{\mathrm{prf}} + q^2/2^n$
CTR\$\$	Random IV for each block	

Cipher block chaining (CBC) $C_0 = \mathrm{IV}$, $C_i = F_k(C_{i-1} \oplus m_i)$

Dec requires being able to calculate F^{-1}.

If F is a (t, q, ε)-secure PRF, then CBC$[F]$ is $(\approx t, \sigma = qn, 2\varepsilon + q^2/2^n)$-ind-cpa-secure. The proof requires showing that for U, all inputs to U are distinct (minus a birthday term).

8 Message authentication code (MAC)

Alice sends message m and $t \leftarrow \mathsf{Tag}_k(m)$. Eve intercepts (m, t) and delivers (m', t') to Bob. Bob runs $\mathsf{Ver}_k(m', t')$.

$$\mathsf{Ver}_k \text{ returns } \begin{cases} m & \text{if } t' \text{ is a valid tag } (\mathsf{Ver}_k \text{ “accepts”}) \\ \perp & \text{otherwise } (\mathsf{Ver}_k \text{ “rejects”}) \end{cases}$$

Eve has access to a Tag_k oracle and can make many attempts on Ver. Eve “wins” if Ver accepts on an m' not previously queried to Tag_k.

Conerns ignored by this model

Dropped messages

Replay attacks (“freshness” of messages)

Message sequence

Unforgeability under chosen message attack

$$\mathrm{Adv}^{\mathrm{ufmca}}_{\mathrm{MAC}}(\mathcal{A}) \equiv \Pr_{k \leftarrow \mathsf{Gen}} \left[\mathcal{A}^{\mathsf{Tag}_k, \mathsf{Ver}_k} \text{ “wins” } \right]$$

MAC is $(t, q_t, q_v, \varepsilon)$-uf-cma-secure iff advantage of an attacker bounded by time t, number of Tag queries q_t, and number of Ver queries q_v is less than ε.

Examples of reasonable constants

t	2^{80} or 2^{128}
q_v, q_t	2^{40} or 2^{56}
ε	2^{-40} or 2^{-56}

Brute-force MAC attacks

Key search: Get a few oracle tags, and guess k. $\mathrm{Adv} = t/2^{\ell}$.

Tag search: $\mathrm{Adv} = t/2^{s}$ where s is the tag length.

PRF-based MAC $\mathsf{Tag}_k \equiv F_k$

$\forall$ (t, q_t, q_v)-bounded $\mathcal{B}$, $\exists$ $(\approx t, q_t + q_v)$-bounded $\mathcal{A}$ such that

$$\mathrm{Adv}^{\mathrm{ufcma}}_{\mathrm{PRFMAC}[F]}(\mathcal{B}) \leq \mathrm{Adv}^{\mathrm{prf}}_{F}(\mathcal{A}) + q_v/2^n \ .$$

CBC-MAC For a fixed t, and $F : \{\mathtt{0},\mathtt{1}\}^{nt} \rightarrow \{\mathtt{0},\mathtt{1}\}^{n}$, CBC-MAC$[F]$ is secure, losing $(qt)^2/2^n$ advantage from that of F.

Cipher-based MAC (CMAC) Adds an extra step to the end of CBC-MAC to make it secure for arbitrary-length messages.

Precompute k_1, $k_2 \in \{\mathsf{0},\mathsf{1}\}^n$ using $F_k(\mathsf{0}^m)$.

$$m'_t \leftarrow \begin{cases} m'_t \oplus k_1 & : |m'_t| = n \\ m' \| \mathsf{000}\ldots \oplus k_2 & : |m'_t| < n \end{cases}$$

Run $m_1 \| \ldots \| m_t$ through CBC-MAC.

9 Combining authenticity and privacy

Integrity of ciphertexts (INT-CTXT) $\mathsf{Dec}_k(c)$: returns decryption of c, or $\perp$ if c is invalid.

$SE = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is INT-CTXT secure iff $\forall$ bounded $\mathcal{A}$,

$$\mathrm{Adv}^{\text{int-ctxt}}_{SE}(\mathcal{A}) \equiv \Pr_{k \leftarrow \mathsf{Gen}} \left[\mathcal{A}^{\mathsf{Enc}_k, \mathsf{Dec}_k} \text{ wins} \right] < \varepsilon \,.$$

UF-CMA-security does not necessarily give INT-CTXT security. For example: If the output of Tag has a spurious bit that is ignored by Ver. So we require a stronger condition:

Strong unforgeability (SUF-CMA) Winning is redefined as: Ver_k accepts (m', t') that was not previously a query/answer pair to Tag_k.

Bad idea: Encrypt-and-tag $\mathsf{AEnc} \equiv \mathsf{EEnc}_{k_e}(m) \| \mathsf{Tag}_{k_m}(m)$. The tag could reveal information about m.

Bad idea: Tag-then-encrypt $\mathsf{AEnc} \equiv \mathsf{EEnc}_{k_e}(m \| \mathsf{Tag}_{k_m}(m))$. The ciphertext might be forgeable (for example, if EEnc appends a spurious bit).

Good idea: Encrypt-then-tag $\mathsf{AEnc} \equiv \mathsf{EEnc}_{k_e}(m) \| \mathsf{Tag}_{k_m}(\mathsf{EEnc}_{k_e}(m))$.

Indistinguishability under chosen ciphertext attack (IND-CCA) IND-CPA $\wedge$ INT-CTXT $\Rightarrow$ IND-CCA.

10 Summary of symmetric crypto games

		Oracles	Goal
Stronger ↓	IND-CPA	L/R	Left or right?
	IND-CCA	L/R, $\widehat{\mathsf{Dec}}$	
Stronger ↓	INT-PTXT	Enc, D	D returns new plaintext
	INT-CTXT		D returns non-$\perp$ on new ciphertext
Stronger ↓	UF-CMA	Tag, Ver	$\mathsf{Ver}(m, t)$: m has never been tagged
	SUF-CMA		$\mathsf{Ver}(m, t)$: (m, t) has never been a Tag pair

11 Hashing

Hash function $h : D \to \{\mathtt{0}, \mathtt{1}\}^n$, $D > 2^n$

Collision $x, x' \in D : h(x) = h(x') \wedge x \neq x'$

Hash family $H : \{\mathtt{0}, \mathtt{1}\}^\ell \times D \to \{\mathtt{0}, \mathtt{1}\}^n$

Collision resistance (CR) H is (t, ε)-collision resistant if $\mathrm{Adv}_H^{\mathrm{cr}}(\mathcal{A}) \leq \varepsilon$ $\forall$ t-bounded $\mathcal{A}$.

$$\mathrm{Adv}_H^{\mathrm{cr}}(\mathcal{A}) = \Pr_{k \leftarrow \{\mathtt{0},\mathtt{1}\}^\ell} [\ \mathcal{A}(k) \text{ outputs a collision in } H_k\ ]$$

Real-world hash functions	MD4	$n = 128$	Broken
	MD5	$n = 128$	Broken
	SHA-1	$n = 160$	Maybe broken
	SHA-256	$n = 256$	Good
	SHA-3		Good

Hash output lengths need to be longer than encryption key lengths because brute-force attacks can test $\approx q^2$ pairs in q hashes ("birthday attack").

Second preimage resistance / target collision resistance (TCR) Given x, attacker must find x' such that x, x' is a collision.

$$\mathrm{Adv}_H^{\mathrm{tcr}}(\mathcal{A}) = \Pr_{\substack{k \leftarrow \{\mathtt{0},\mathtt{1}\}^\ell, \\ x \leftarrow D}} [\ \mathcal{A}(k, x) \text{ outputs a collision}\ ]$$

where D is some distribution over the message space.

Brute force attack does not have a birthday advantage in this game.

CR ⇒ TCR.

One-wayness (OW)

$$\mathrm{Adv}_H^{\mathrm{ow}}(\mathcal{A}) = \Pr_{\substack{k \leftarrow \{\mathtt{0},\mathtt{1}\}^\ell, \\ x \leftarrow D}} \left[\ \mathcal{A}(k, H_k(x)) \text{ outputs } x' : H_k(x') = H_k(x)\ \right]$$

TCR ⇒ OW for "high-entropy" D (so that $H_k(x)$ reveals very little about x).

Merkle-Damgård (MD) transform $\mathrm{MD}[h]_k(M \in \{\mathtt{0},\mathtt{1}\}^*)$

Uses a compression function $h_k : \{\mathtt{0},\mathtt{1}\}^\ell \times \{\mathtt{0},\mathtt{1}\}^{b+n} \to \{\mathtt{0},\mathtt{1}\}^n$

Break M into $M_1, \ldots, M_t$ s.t. $\|M_i\| = b$

$$\begin{aligned}
y_1 &\leftarrow h_k(\ M_1 \,\|\, \langle 0 \rangle\ ) \\
y_2 &\leftarrow h_k(\ M_2 \,\|\, y_1\ ) \\
&\vdots \\
y_i &\leftarrow h_k(\ M_i \,\|\, y_{i-1}\ ) \\
&\vdots \\
y_t &\leftarrow h_k(\ M_t \,\|\, y_{t-1}\ ) \\
y &\leftarrow h_k(\ \langle t \rangle \,\|\, y_t\ )
\end{aligned}$$

If *h* is CR, then MD[h] is CR Let $\mathcal{B}$ attack MD$[h]$ in CR game. We can build $\mathcal{A}$ attacking h in CR game. $\mathcal{A}(k \in \{\mathtt{0},\mathtt{1}\}^\ell)$ will use a collision x, x' in MD$[h_k]$ to find a collision in h_k.

If x, x' have different numbers of blocks: Then $\langle t \rangle \,\|\, M_t, \langle t' \rangle \,\|\, M'_t$ is a collision in h_k.

Otherwise: Walk backward through the MD process to find a step where $M_i \,\|\, y_{i-1} \neq M'_i \,\|\, y'_{i-1}$.

HMAC Secure MAC based on hash function.

$\mathrm{HMAC}_k(m) = H((k \oplus \mathrm{opad}) \,\|\, H((k \oplus \mathrm{ipad}) \,\|\, m))$ where k is the MAC key padded to the length of the compression function, ipad and opad are fixed strings of the same length.

Only TCR security of H is required for the security of HMAC.

12 Groups

Group axioms

G is closed under $\cdot$

$\mathbb{1} \cdot a = a \cdot \mathbb{1} = a$

Every element of G has a unique multiplicative inverse

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

The group operator $\cdot$ is not necessarily commutative.

Examples of groups

Integers under addition

Invertible matrices with real entries under multiplication

$\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ under modular addition

$\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N : \gcd(a, N) = 1\}$ under multiplication $\pmod N$

$\mathbb{Z}_N^*$ is closed under $\cdot$ Proof sketch:
$\gcd(a \cdot b, N) = 1 \implies \gcd(ab \bmod N, N) = 1$.

$\mathbb{Z}_N^*$ has unique inverses Proof sketch:
Use the fact $\gcd(a, N) = 1 \iff \exists\, x, y \in \mathbb{Z} : ax + Ny = 1$.
$ax = 1 - Ny = 1 \mod N \implies x = a^{-1} \mod N$.

Generator $g \in G : \{g^0, g^1, g^2, \ldots\} = G$
If G is finite, then $a^{|G|} = 1\ \forall\, a \in G$.
g is a generator iff $g^i \neq \mathbb{1}\ \forall\ 0 < i < |G| : i \mid G$
For a prime p, $\mathbb{Z}_p^*$ is finite and cyclic (has a generator). Its order is $p-1$.

Order of $a \in G$ is $(\min i > 0 : a^i = 1)$.
order(a) divides $|G|$.

How many generators? If $g \in G$ is a generator and i is coprime with $|G|$, then g^i is a generator. Therefore we have $\left|\mathbb{Z}_{p-1}^*\right|$ generators.

13 Diffie-Hellman protocol (1976)

For establishing a secret key without meeting.

A chooses $a \in G$ and transmits g^a. B chooses $b \in G$ and transmits g^b. The secret is g^{ab}.

Requires a multiplicative group $(G, \cdot)$ and a generator $g \in G$, and the discrete log problem must be intractable.

Calculations required for implementation Multiply huge numbers ($\approx 2^{4096}$), exponentiate huge numbers, sample huge primes, find a generator of $\mathbb{Z}_p^*$.

Multiplication Simple grade-school multiplication algorithm followed by Euclid's division algorithm. Both are quadratic in bit length.

Exponentiation Repeated squaring. $O(\lg^3 a)$ multiplications.

Primality testing Miller-Rabin test runs in $O(\lg^3 p)$, randomized with false positives. Alternately, AKS is a deterministic test running in $O(\lg^6 p)$. Approximately $1/k$ of k-bit numbers are prime.

Generator testing g is a generator if $g^{(p-1)/i} = 1$ $\forall$ prime divisors i of $p-1$. Since factoring is hard, we must generate p such that we know the factors of $p-1$ ...

Sophie Germain (safe) primes Pick a prime q and let $p = 2q + 1$. Repeat until p is prime. It appears that $1/k^2$ of k-bit numbers are safe primes, although this is unproven.

Uniformity of shared secret We want $ab \bmod (p-1)$, and therefore also g^{ab}, to be uniformly distributed. If $G = \mathbb{Z}_p^*$, this is not the case; ab is even with probability $3/4$, and the $\bmod (p-1)$ operation does not affect this parity (because $p-1$ is even). But if G has prime order q, then $ab \bmod q$ is very nearly uniform ($ab = 0$ with probability $2/q$, anything else with probabilility $1/(q-1)$).

Quadratic residue The subgroup of quadratic residues in $\mathbb{Z}_p^*$ is $\mathbb{QR}_p^* = \{(g^2)^0, (g^2)^1, (g^2)^2, \ldots, (g^2)^{(p-3)/2}\}$. For $p = 2q+1$, $\left|\mathbb{QR}_p^*\right| = q$, so if p is a safe prime, $\left|\mathbb{QR}_p^*\right|$ has prime order. g^2 is a generator for $\mathbb{QR}_p^*$.

Jacobi symbol For $y \in \mathbb{Z}_p^*$, Jacobi symbol is 1 if $y \in \mathbb{QR}_p^*$, and -1 otherwise. $y \in \mathbb{QR}_p^* \iff y^{(p-1)/2} = 1$. Proof: $y^{(p-1)/2} = g^{i(p-1)/2}$ for some $i = 2i' + b$, $b \in \{0, 1\}$. Use the fact that $g^{(p-1)/2} = -1$. $y = g^{b(p-1)/2} = \{1 \text{ if } b = 0, \ -1 \text{ if } b = 1\}$.

14 Asymmetric encryption

Scheme AE = (Gen, Enc, Dec)

$(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathsf{Gen}$

$c \leftarrow \mathsf{Enc}_{\mathrm{pk}}(m) = \mathsf{Enc}(\mathrm{pk}, m)$ where $m \in M_{\mathrm{pk}}$, and M_{pk} is some group

m or $\perp \leftarrow \mathsf{Dec}_{\mathrm{sk}}(c)$

Gen and Enc are randomized. Dec is deterministic.

IND-CPA-security

$$\mathrm{Adv}_{\mathrm{AE}}^{\mathrm{indcpa}}(\mathcal{A}) \equiv \Pr_{(\mathrm{pk},\mathrm{sk}) \leftarrow \mathsf{Gen}} \left[\mathcal{A}^{L_{\mathrm{pk}}}(\mathrm{pk})\right] - \Pr_{(\mathrm{pk},\mathrm{sk}) \leftarrow \mathsf{Gen}} \left[\mathcal{A}^{R_{\mathrm{pk}}}(\mathrm{pk})\right]$$

where $L_{\mathrm{pk}}(m_L, m_R) = \mathsf{Enc}_{\mathrm{pk}}(m_L)$ and $R_{\mathrm{pk}}(m_L, m_R) = \mathsf{Enc}_{\mathrm{pk}}(m_R)$.

IND-CCA-security Like IND-CPA, but the attacker gets another oracle:

$$D_{\mathrm{sk}}(c) = \begin{cases} \mathsf{Dec}_{\mathrm{sk}}(c) & \text{if } c \text{ was not returned by L/R oracle} \\ \perp & \text{otherwise} \end{cases}.$$

One encryption query $\forall$ ind-cpa attacker $\mathcal{B}$ against AE, $\exists$ an ind-cpa attacker $\mathcal{A}$ against AE making $\leq q$ Enc queries such that $\mathrm{Adv}_{\mathrm{AE}}^{\mathrm{indcpa}}(\mathcal{B}) \leq q \, \mathrm{Adv}_{\mathrm{AE}}^{\mathrm{indcpa}}(\mathcal{A})$. (Also, same for ind-cca with 1 encryption query and unlimited D_{sk} queries.) The analogous claim is not true in a symmetric key setting.

ElGamal Asymmetric encryption scheme similar to Diffie-Hellman.

Gen: Choose group G of order n, generator g. Choose $x \leftarrow \mathbb{Z}_n$. Output $(\mathrm{sk} = x, \mathrm{pk} = (G, G, X = g^x))$.

$\mathsf{Enc}_{\mathrm{pk}}(m \in G)$: Choose $y \leftarrow \mathbb{Z}_n$. Output $c = (Y = g^y, \overbrace{m \cdot X^y}^{g^{xy}})$.

$$\mathsf{Dec}_{\mathsf{sk}}(\overbrace{Y}^{g^y}, \overbrace{Z}^{m \cdot g^{xy}})\text{: Output } \overbrace{Z}^{m \cdot g^{xy}} \cdot (\overbrace{Y^x}^{g^{xy}})^{-1} = m.$$

Not ind-cpa-secure for $G = \mathbb{Z}_p^*$. Attack: $(Y, Z) \leftarrow O(1, g)$. Accept if $Z^{(p-1)/2} = 1$, reject if -1. $\Pr[\mathcal{A}^L] = \Pr[1 \cdot g^{xy} \text{ is square}] = 3/4$. $\Pr[\mathcal{A}^R] = \Pr[g^{xy+1} \text{ is square}] = 1/4$.

Is ind-cpa-secure under assumption that DDH (decision Diffie-Hellman) is hard.

Is not cca-secure. But the Cramer-Shoup scheme is, using two applications of ElGamal, under the DDH assumption.