T-79.5502 Advanced Course in Cryptology

Lecture 3, Nov 8, 2007

Insecurity of textbook crypto (Chapter 8)

- Weak security notion
- The CDH and DL Problems and Assumptions
- Cryptanalytic attacks against Public Key Cryptosystems
- RSA Problem and Assumption
- IF Problem and Assumption
- Active attack on textbook RSA
- Insecurity of Rabin encryption
- All-or-nothing secrecy of ElGamal encryption

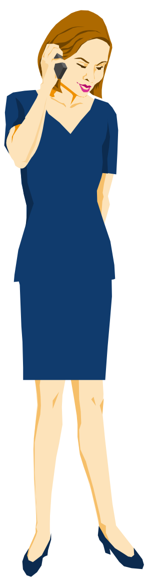
Weak Security Notion (Property 8.2)

(i) All-or-nothing secrecy: For a given ciphertext output from a given encryption algorithm, the attacker's task is to retrieve the whole plaintext block; or for a given plaintext-ciphertext pair the attacker's task is to uncover the secret key. The attacker either succeeds to get all of the secret or fails with nothing.

(ii) The attacker does not manipulate or modify ciphertexts , and does not ask a key owner to provide encryption or decryption services.

Diffie-Hellman Key Exchange

ALICE



$a \in_U [1, p\text{-}1]$

$A = g^a \mod p$

$K = B^a \mod p$

A →

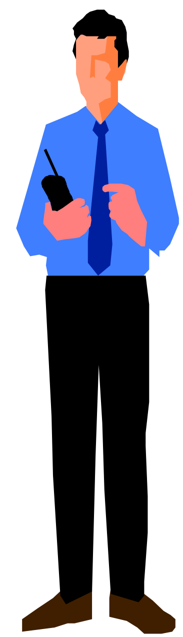
← B

BOB

$b \in_U [1, p\text{-}1]$

$B = g^b \mod p$

$K = A^b \mod p$



Security of Diffie-Hellman Key Exchange

- If the Discrete Logarithm Problem (DL) is easy then DH KE is insecure
- Computational Diffie-Hellman Problem (CDH):

  Given g, g^a, g^b, compute g^{ab}.
- It seems that in groups where the CDH is easy, also the DL is easy. It is unknown if this holds in general (Maurer-Wolf).
- DH KE is secure against passive wiretapping.
- DH KE is insecure under the active man-in-the-middle attack: Man-in-the-Middle exchanges a secret key with Alice, and another with Bob, while Alice believes that she is talking confidentially to Bob, and Bob believes he is talking confidentially to Alice (see next slide).
- This problem is solved by authenticating the Diffie-Hellman key exchange messages.

Man-in-the-Middle in the DH KE

Alice		Malice (man-in-the-middle)		Bob
a		c_1		
g^a	$\xrightarrow{g^a}$	g^{c1}	$\xrightarrow{g^{c1}}$	b
			$\xleftarrow{g^b}$	g^b
		c_2		
	$\xleftarrow{g^{c2}}$	g^{c2}		
$K_2 = (g^a)^{c2}$		$K_1 = (g^b)^{c1}$		$K_1 = (g^b)^{c1}$
		$K_2 = (g^a)^{c2}$		
	Protection using K_2 $\longleftrightarrow$		Protection using K_1 $\longleftrightarrow$	

CDH and DL Problems (in a finite group)

Definition 8.1 CDH Problem

INPUT $\mathrm{desc}(G)$: the description of finite group G

$g \in G$: a generator element of g

$g^a, g^b \in G$ for some integers $0 < a,b < \mathrm{ord}\,(G)$

OUTPUT g^{ab}

Definition 8.2: DL Problem

INPUT $\mathrm{desc}(G)$: the description of finite group G

$g \in G$: a generator element of g

$h \in_{\mathrm{U}} G$

OUTPUT the unique integer $a < \mathrm{ord}(G)$ such that $h = g^a$

(denote $a = \log_g h$)

CDH Assumption (in a finite group)

Assumption 8.1 CDH Assumption

A CDH problem solver is a $\mathcal{PP}$ algorithm $\mathcal{A}$ with an advantage $\varepsilon > 0$ defined by $\varepsilon = \mathrm{Prob}[\, g^{ab} \leftarrow \mathcal{A}(\mathrm{desc}(G), g, g^a, g^b\,)]$, where the input to $\mathcal{A}$ is given in Def 8.1. and the probability is taken over random choices of G, g, a and b.

Let $\mathcal{IG}$ be an instance generator that on input 1^k runs in time polynomial in k and outputs

(i) $\mathrm{desc}(G)$ with $\mathrm{ord}\,(G) = q$, where $|q| = k$,

(ii) a generator element $g \in G$,

(iii) g^a and g^b , where a and b in $(0, q]$.

We say that $\mathcal{IG}$ satisfies the Computational Diffie-Hellman (CDH) assumption, if there is no CDH problem solver for $\mathcal{IG}(1^k)$ with advantage $\varepsilon(k) > 0$ that is non-negligible in k, for all sufficiently large k.

The difficulty of the CDH problem means that Diffie-Hellman KE is secure (the key remains secret) under passive attacks.

Recall: Non-Polynomial Bounds

Definition 4.12. A function $f(n)\colon \mathbb{N} \to \mathbb{R}$ is said to be unbounded by any polynomial in n (or, non-polynomially bounded quantity) if for any polynomial $p(n)$ there exists a natural number n_0 such that $f(n) > p(n)$, for all $n > n_0$.

Definition 4.13. A function $\varepsilon(n)\colon \mathbb{N} \to \mathbb{R}$ is said to be a negligible in n if its inverse $1/\varepsilon(n)$ is a non-polynomially bounded quantity.

Hence a function $\varepsilon(\mathrm{n})\colon \mathbb{N} \to \mathbb{R}$ is said to be a non-negligible in n if its inverse $1/\varepsilon(n)$ is a polynomially bounded quantity.

DL Assumption (in a finite group)

Assumption 8.1 DL Assumption

A DL problem solver is a $\mathcal{PP}$ algorithm $\mathcal{A}$ with advantage $\varepsilon > 0$ defined by $\varepsilon = \mathrm{Prob}[\, \log_g h \leftarrow \mathcal{A}(\mathrm{desc}(G), g, h\,)]$ where the input to $\mathcal{A}$ is defined in Def 8.2. and the probability is taken over random choices of G, g and h.

Let $\mathcal{IG}$ be an instance generator that on input 1^k runs in time polynomial in k and outputs

(i) $\mathrm{desc}(G)$ with $\mathrm{ord}\,(G) = q$, where $|q| = k$,

(ii) a generator element $g \in G$,

(iii) $h \in G$.

We say that $\mathcal{IG}$ satisfies the Discrete Logarithm (DL) assumption if there is no DL problem solver for $\mathcal{IG}(1^k)$ with advantage $\varepsilon(k) > 0$ that is non-negligible in k for all sufficiently large k.

If DL Assumption holds then the function $x \rightarrow g^x$ is one way. It is not known if it is a trap-door one-way function.

Trapdoor One-way Function

Property 8.1:

A one-way trapdoor function is a one-way function f_t: $D \rightarrow R$, i.e., it is *easy* to evaluate for all $x \in D$ and *difficult* to invert, for almost all values in R. However, if the trapdoor information is used, then for all values $y \in R$ it is *easy* to compute $x \in D$ satisfying $y = f_t(x)$.

easy = there is an practically efficient algorithm and an non-negligible advantage to get the result right

difficult = not easy

Importance of Arbitrary Instances for Intractability Assumptions

For example: If the order q of the group G is a smooth number, i.e.,

$$q = q_1^{e1} q_2^{e2} \ldots q_m^{em}$$

then we can find the discrete logarithm efficiently using the Pohlig-Hellman algorithm. Actually, we solve the discrete logarithm problem separately in each small group of order q_i^{ei} generated by g^{ri} where

$$ri = q/q_i^{ei}$$

(Recall the structure of a finite cyclic group. Example: If g is a generator of $\mathbb{Z}^*_{19}$, g is of order $18 = 2 \cdot 3^2$, then $g_1 = g^2$ is a generator of a cyclic subgroup of order 9 and $g_2 = g^9$ is a generator of cyclic subgroup of order 2 in $\mathbb{Z}^*_{19}$. For each $h \in \mathbb{Z}^*_{19}$ the discrete logarithm $a = \log_g h$ *can* be found by computing $a_1 = \log_{g1} h^2 = 2a \bmod 9$ and $a2 = \log_{g2} h^9 = 9a \bmod 2$ and combining the results using the Chinese Remainder Theorem).

Cryptanalysis against PK cryptosystems: Active Attacks

Chosen-plaintex attack (CPA): An attacker has the encryption black box in its possession.

Chosen-ciphertext attack (CCA): An attacker can give a finite number of ciphertexts (excl. the target ciphertext) and see the corresponding decryptions.

Adaptive chosen-ciphertext attack (CCA2): An attacker has the decryption black box in its possession, and can input chosen ciphertexts (excl. the target one) and obtain the decryptions, one at a time.

The RSA Problem and Assumption

Definition 8.4 RSA Problem

INPUT $N = pq$ with p, q prime numbers

e: an integer such that $\gcd(e, \phi(N)) = 1$

$c \in \mathbf{Z}_N^*$

OUTPUT the unique integer $m \in \mathbf{Z}_N^*$ such that $m^e \equiv c \pmod N$

Assumption 8.3 RSA Intractability Assumption

An RSA problem solver is a $\mathcal{PP}$ algorithm $\mathcal{A}$ with an advantage $\varepsilon > 0$ defined by $\varepsilon = \mathrm{Prob}[\, m \leftarrow \mathcal{A}(N, e, m^e)]$ where the input to $\mathcal{A}$ is defined in Def 8.4.

Let $\mathcal{IG}$ be an instance generator that on input 1^k runs in time polynomial in k and outputs

(i) a $2k$-bit modulus $N = pq$ where p and q are two distinct uniformly random primes each is k bits long

(ii) $e \in \mathbf{Z}^*_{(p-1)(q-1)}$

We say that $\mathcal{IG}$ satisfies the RSA assumption if there is no RSA problem solver for $\mathcal{IG}(1^k)$ with advantage $\varepsilon(k) > 0$ non-negligible in k, for all sufficiently large k.

The Integer Factorization Problem and Intractability Assumption

Definition 8.5 IF Problem

INPUT N odd composite integer with at least two distinct prime factors

OUTPUT prime p such that $p \mid N$

Assumption 8.4 IF Assumption

An IF problem solver is a $\mathcal{PP}$ algorithm $\mathcal{A}$ with an advantage $\varepsilon > 0$ defined by $\varepsilon = \text{Prob}[\ \mathcal{A}(N) \text{ divides } N \text{ and } 1 < \mathcal{A}(N) < N]$ where the input to $\mathcal{A}$ is defined in Def 8.5.

Let $\mathcal{IG}$ be an instance generator that on input 1^k runs in time polynomial in k and outputs a $2k$-bit modulus $N = pq$ where p and q are two distinct uniformly random primes each is k bits long.

We say that $\mathcal{IG}$ satisfies the IF assumption if there is no IF problem solver for $\mathcal{IG}(1^k)$ with advantage $\varepsilon > 0$ non-negligible in k for all sufficiently large k.

An Attack on the Text-book RSA

Recall: Multiplicative property of the RSA

Attack: Malice sees c and knows that $m < 2^t$. With non-negligible probability there exist m_1 and m_2 such that $m = m_1 \cdot m_2$, where $m_1 < 2^{t/2}$.

Hence $c = m_1^e \cdot m_2^e \pmod{N}$.

Malice builds a list $\{1^e, 2^e, 3^e, \ldots, (2^{t/2})^e\}$

And searches through the sorted list trying to find i and $j \in \{1, 2, 3, \ldots, 2^{t/2}\}$ such that

$$c \cdot (i^e)^{-1} \equiv j^e \pmod{N}$$

Cost

Space cost: $2^{t/2} \cdot \log N$ bits

Time cost:

- creating lists $O_{\mathrm{B}}(2^{t/2} \cdot \log^3 N)$
- sorting the list $O_{\mathrm{B}}(t/2 \cdot 2^{t/2})$
- searching through the sorted list $O_{\mathrm{B}}(2^{t/2} \cdot (t/2 + \log^3 N))$

Total time cost: $O_{\mathrm{B}}(2^{t/2+1} \cdot (t/2 + \log^3 N))$

If the space cost is affordable then the attack achieves square root level reduction in time complexity.

Real life instantiation: m = DES-key, $t = 56$, space 2^{38} bits, time 2^{29} modular exponentiations.

Insecurity of Rabin

All-or-nothing security of Rabin encryption is equivalent to the intractability of the IF problem. For a proof see Stinson's book (T-79.5501).

However, Rabin encryption is not secure under CCA attack:

given a decryption oracle, there is an efficient algorithm to compute square roots. Given an algorithm to compute square roots there a probabilistic algorithm to factorise the modulus.

See also Lecture 1, Slide 13 (Rabin OT)

Security of ElGamal encryption

Theorem 8.3 For a plaintext message uniformly distributed in the plaintext message space, the ElGamal cryptosystem is "all-or-nothing" secure against CPA if and only if the CDH is hard.

Proof: "<=" Assume ElGamal is not "all-or-nothing" secure. Then there is a decryption oracle, which given public key (p, g, y) and ciphertext (c_1,c_2), the oracle outputs

$$m \leftarrow (p,g,y, c_1,c_2)$$

with a non-negligible advantage δ, such that

$$c_2 /m \equiv g^t \,(\text{mod } p),$$ where $t = (\log_g y)(\log_g c_1)$.

Then for an arbitrary CDH problem instance (p,g, g_1,g_2) we set (p,g, g_1) as the public key and set (g_2, c_2) as ciphertext pair for a random c_2 .

Then with advantage δ, the ElGamal decryption oracle outputs

$$m \leftarrow (p, g, g_1, g_2, c_2)$$

with m satisfying

$$c_2 /m \equiv g^{ab}(\text{mod } p),$$ where $a = \log_g g_1$ and $b = \log_g g_2$

thus solving the CDH problem efficiently.

Insecurity of ElGamal encryption

Consider the case $G = \mathbb{Z}_p^*$, where p is prime. Then q divides p -1. From the ciphertext, Malice gets

$$c_2^q = m^q$$

where q is the order of the generator g. This gives information about m if m is not in the subgroup, and makes ElGamal encryption deterministic!

ElGamal encryption is multiplicative. Hence the same attack as with the RSA applies. The time complexity of the attack is about $2^{q/2}$.

Summary – Intractability Assumption

1. *Security parameter* 1^k , $k \in \mathbb{N}$, e.g., $k = 160$
2. *Problem* with instance space $\mathcal{I}$ and solution space $\mathcal{S}$
3. *Instance generator* $\mathcal{IG}$: $\mathbb{N} \to \mathcal{I}$
4. *Problem solver* $\mathcal{SG}$*:* $\mathcal{I} \to \mathcal{S}$ with advantage ε: $\mathbb{N} \to (0,1]$,

   $\varepsilon(k) = \Pr[S = \mathcal{SG}(I)$ is a solution to the problem, for $I = \mathcal{IG}(k)]$,

   where the probability is taken over the randomness of $\mathcal{IG}$ and $\mathcal{SG}$.
5. We say that $\mathcal{IG}$ satisfies intractability assumption for this problem, if there is no solver $\mathcal{SG}$ with non-negligible advantage. This means that there is no solver with advantage $\varepsilon = \varepsilon(k)$ and no polynomial $p(k)$ such that there exists k_0 such that $1/\varepsilon(k) < p(k)$, for $k > k_0$.