Introduction to Cryptology

Lecture 22
Announcements

• HW10 due today
• HW11 posted on course webpage. Due on 5/7.
  – We will have 12 homeworks total. The 2 lowest homework grades will be dropped.
Agenda

• Last time:
  – Number Theory and Cryptographic Assumptions (8.3)

• This time:
  – Key Exchange Definition, Diffie-Hellman Key Exchange (10.3)
  – Public Key Encryption Definitions (11.2)
  – El Gamal Encryption (11.4)
  – RSA Encryption (11.5)
Key Agreement

The key-exchange experiment $KE_{A,\Pi}^{eav}(n)$:

1. Two parties holding $1^n$ execute protocol $\Pi$. This results in a transcript $\text{trans}$ containing all the messages sent by the parties, and a key $k$ output by each of the parties.

2. A uniform bit $b \in \{0,1\}$ is chosen. If $b = 0$ set $\hat{k} := k$, and if $b = 1$ then choose $\hat{k} \in \{0,1\}^n$ uniformly at random.

3. $A$ is given $\text{trans}$ and $\hat{k}$, and outputs a bit $b'$.

4. The output of the experiment is defined to be 1 if $b' = b$ and 0 otherwise.

Definition: A key-exchange protocol $\Pi$ is secure in the presence of an eavesdropper if for all ppt adversaries $A$ there is a negligible function $neg$ such that

$$\Pr[KE_{A,\Pi}^{eav}(n) = 1] \leq \frac{1}{2} + neg(n).$$
Diffie-Hellman Key Exchange

\[ x \leftarrow \mathbb{Z}_q \]
\[ h_1 := g^x \]
\[ \underline{\mathbb{G}, q, g, h_1} \]
\[ y \leftarrow \mathbb{Z}_q \]
\[ h_2 := g^y \]
\[ k_A := h_2^x \]
\[ k_B := h_1^y \]

**FIGURE 10.2:** The Diffie-Hellman key-exchange protocol.
Security Analysis

Theorem: If the DDH problem is hard relative to $G$, then the Diffie-Hellman key-exchange protocol $\Pi$ is secure in the presence of an eavesdropper.
Recall DDH problem

We say that the DDH problem is hard relative to $G$ if for all ppt algorithms $A$, there exists a negligible function $neg$ such that

\[
\left| \Pr[A(G, q, g, g^x, g^y, g^z) = 1] - \Pr[A(G, q, g, g^x, g^y, g^{xy}) = 1] \right| \leq neg(n).
\]
Security Reduction

Assume DH key-exchange protocol is insecure. Then, there exists a ppt adversary $A$ such that

$$\Pr\left[K_{E_{A,\Pi}}^eav(n) = 1\right] \geq \frac{1}{2} + \epsilon(n),$$

for non-negligible $\epsilon$. We construct the following adversary $A'$ breaking the DDH assumption.

$A'$ does the following: On input $(G, q, g, h_1, h_2, h_3)$, $A'$ sets $\text{trans} := (G, q, g, h_1, h_2)$ and sets $\hat{k} := h_3$. $A'$ runs $A(\text{trans}, \hat{k})$ and returns whatever $A$ returns.
Security Analysis

Case 1: \((G, q, g, h_1, h_2, h_3) = (G, q, g, g^x, g^y, g^z)\)
\[\Pr[A'(G, q, g, g^x, g^y, g^z) = 1] = \Pr[KE_{eav}^{A,\Pi}(n) = 1|b = 1]\]

Case 2: \((G, q, g, h_1, h_2, h_3) = (G, q, g, g^x, g^y, g^{x\cdot y})\)
\[\Pr[A'(G, q, g, g^x, g^y, g^{x\cdot y}) = 1] = \Pr[KE_{eav}^{A,\Pi}(n) = 0|b = 0] = 1 - \Pr[KE_{eav}^{A,\Pi}(n) = 1|b = 0].\]

Thus, \(\frac{1}{2} |\Pr[A'(G, q, g, g^x, g^y, g^z) = 1] - \Pr[A'(G, q, g, g^x, g^y, g^{x\cdot y}) = 1]| = \Pr[KE_{eav}^{A,\Pi}(n) = 1] - \frac{1}{2} \geq \epsilon(n).\)

And so
\[|\Pr[A'(G, q, g, g^x, g^y, g^z) = 1] - \Pr[A'(G, q, g, g^x, g^y, g^{x\cdot y}) = 1]| \geq 2\epsilon(n),\]
which is non-negligible.
This is a contradiction to the DDH assumption.
Public Key Encryption

Definition: A public key encryption scheme is a triple of ppt algorithms $(Gen, Enc, Dec)$ such that:

1. The key generation algorithm $Gen$ takes as input the security parameter $1^n$ and outputs a pair of keys $(pk, sk)$. We refer to the first of these as the public key and the second as the private key. We assume for convenience that $pk$ and $sk$ each has length at least $n$, and that $n$ can be determined from $pk, sk$.

2. The encryption algorithm $Enc$ takes as input a public key $pk$ and a message $m$ from some message space. It outputs a ciphertext $c$, and we write this as $c \leftarrow Enc_{pk}(m)$.

3. The deterministic decryption algorithm $Dec$ takes as input a private key $sk$ and a ciphertext $c$, and outputs a message $m$ or a special symbol $\perp$ denoting failure. We write this as $m := Dec_{sk}(c)$.

Correctness: It is required that, except possibly with negligible probability over $(pk, sk)$ output by $Gen(1^n)$, we have $Dec_{sk}\left(Enc_{pk}(m)\right) = m$ for any legal message $m$. 
CPA-Security

The CPA experiment $PubK_{A,\Pi}^{cpa}(n)$:

1. $Gen(1^n)$ is run to obtain keys $(pk, sk)$.
2. Adversary $A$ is given $pk$, and outputs a pair of equal-length messages $m_0, m_1$ in the message space.
3. A uniform bit $b \in \{0, 1\}$ is chosen, and then a challenge ciphertext $c \leftarrow Enc_{pk}(m_b)$ is computed and given to $A$.
4. $A$ outputs a bit $b'$. The output of the experiment is 1 if $b' = b$, and 0 otherwise.

Definition: A public-key encryption scheme $\Pi = (Gen, Enc, Dec)$ is CPA-secure if for all ppt adversaries $A$ there is a negligible function $neg$ such that

$$Pr \left[ PubK_{A,\Pi}^{cpa}(n) = 1 \right] \leq \frac{1}{2} + neg(n).$$
Discussion

• In the public key setting security in the presence of an eavesdropper and CPA security are equivalent (since anyone can encrypt using the public key).

• CPA-secure encryption cannot be deterministic!!
  – Why not?
Important Property

Lemma: Let $G$ be a finite group, and let $m \in G$ be arbitrary. Then choosing uniform $k \in G$ and setting $k' := k \cdot m$ gives the same distribution for $k'$ as choosing uniform $k' \in G$. Put differently, for any $\hat{g} \in G$ we have

$$\Pr[k \cdot m = \hat{g}] = 1/|G|.$$
El Gamal Encryption Scheme

**CONSTRUCTION 11.16**

Let $G$ be as in the text. Define a public-key encryption scheme as follows:

- **Gen:** on input $1^n$ run $G(1^n)$ to obtain $(G, q, g)$. Then choose a uniform $x \leftarrow \mathbb{Z}_q$ and compute $h := g^x$. The public key is $(G, q, g, h)$ and the private key is $(G, q, g, x)$. The message space is $G$.

- **Enc:** on input a public key $pk = (G, q, g, h)$ and a message $m \in G$, choose a uniform $y \leftarrow \mathbb{Z}_q$ and output the ciphertext

  $$(g^y, h^y \cdot m).$$

- **Dec:** on input a private key $sk = (G, q, g, x)$ and a ciphertext $(c_1, c_2)$, output

  $$\hat{m} := c_2/c_1^x.$$

The El Gamal encryption scheme.
El Gamal Example

• Let the group $G$ be the group of quadratic residues over $\mathbb{Z}_p^*$, where $p$ is a strong prime (i.e. $p = 2q + 1$ for prime $q$).
• $p = 11$, $g = 4$, $x = 3$, $h = 9$, $m = 5$
• $Enc_{(11,5,4,9)}(5)$: Choose $y = 2$
  Output: $c := \langle 5, 4 \cdot 5 \rangle = \langle 5, 9 \rangle$
• $Dec_{(11,5,4,3)}(\langle 5, 9 \rangle) = \frac{9}{5^3} = \frac{9}{4} = 9 \cdot 3 = 27 \mod 11 = 5$. 
Security Analysis

Theorem: If the DDH problem is hard relative to $G$, then the El Gamal encryption scheme is CPA-secure.