18-330 Cryptography Notes: Public Key Cryptography

Note: This is provided as a resource and is not meant to include all material from lectures or recitations. The proofs shown, however, are good models for your homework and exams.

1 Assumptions Related to Discrete Log

We give high-level definitions of standard assumptions related to discrete logarithms.
Let G be a group, and let g be a generator of that group. Both G and g are publicly known.

1. **Discrete Log Assumption**: Given g^x, it is hard to compute x.

2. **Computational Diffie Hellman (CDH) Assumption**: Given g^x, g^y, it is hard to compute g^{xy}.

3. **Decisional Diffie Hellman (DDH) Assumption**: Given g^x, g^y, it is hard to **distinguish** g^{xy} from g^r for a randomly chosen r.

2 Diffie-Hellman Key Exchange

Definition 1. *The **Diffie-Hellman Key Exchange** (DHKE) is an algorithm by which two nodes can collaborate to generate a shared key.*

DHKE is run as follows:

1. *Alice and Bob publicly agree on a large prime p and a generator g, where $0 < g < p$.*

2. *Alice chooses a private key a, and Bob chooses a private key b.*

3. *Alice sends Bob $A = g^a \mod p$, and Bob sends Alice $B = g^b \mod p$.*

4. *Alice calculates $K = B^a \mod p$, and Bob calculates $K = A^b \mod p$.*

We can show that Alice and Bob calculate the same key.
This is Alice's calculation:

$$K = (g^b)^a = g^{ba} = g^{ab} \pmod p$$

Similarly, this is Bob's calculation:

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

With this, it is clear that the two calculations return the same result.

From this exchange, an eavesdropper would only be able to obtain p, g, g^a, and g^b. If the CDH assumption is true for $\mathcal{Z}_p$, then an adversary will not be able to calculate g^{ab}. If Alice and Bob plan to use g^{ab} as a key, however, they will need to make the DDH assumption, since a key is expected to chosen at random, and CDH does not in this case mean that the adversary has no partial information about g^{ab}; he just does not have enough to compute g^{ab} in its entirety.

Although an eavesdropper cannot break DHKE, the protocol is vulnerable to a man-in-the-middle (MitM) attack. DHKE does not authenticate who the other party in the exchange is. That is, if a MitM anticipates that Alice will be talking to Bob in the near future, he could intercept Alice's messages to Bob, and perform the other side of the key exchange on Bob's behalf. Alice would be unaware that she is not talking to the correct person.

3 Public Key Encryption

Definition 2. *A **public key encryption scheme** $\mathcal{E} = (G, E, D)$ defined over $(\mathcal{M}, \mathcal{C})$ is a triple of efficient algorithms: a **key generation algorithm** G, an **encryption algorithm** E, and a **decryption algorithm** D:*

1. *$G()$: A randomized algorithm that outputs a key pair (pk, sk). pk is called the **public key**, while sk is called the **secret key**.*

2. *$E(pk, m)$: A randomized algorithm that takes $m \in \mathcal{M}$ and outputs $c \in \mathcal{C}$, where pk is the public key (as output by G).*

3. *$D(sk, c)$: A deterministic algorithm that takes $c \in \mathcal{C}$ and outputs $m \in \mathcal{M}$ or bot. sk is the secret key (as output by G).*

We require that decryption is the inverse of encryption: For all possible outputs (pk, sk) of G, and all messages m, we have:

$$Pr[D(sk, E(pk, m)) = m] = 1$$

4 IND-CPA Security (Semantic Security)

4.1 IND-CPA Adversarial Game

Definition 3. *Let $\mathcal{E} = (G, E, D)$ be a public key encryption scheme defined over $(\mathcal{M}, \mathcal{C})$. The semantic security game is defined as follows:*

1. *The experiment takes as input bit $b \in \{0, 1\}$, chosen uniformly at random.*

2. *The Challenger runs $(pk, sk) \leftarrow G()$*

3. *The Adversary runs some logic to select any two messages $m_0, m_1 \in \mathcal{M}$, where $|m_0| = |m_1|$.*

4. *The Challenger replies with $E(pk, m_b)$.*

5. *The Adversary outputs a bit $b' \in \{0, 1\}$, which is the output of the experiment.*

4.2 Semantic Security Advantage

Definition 4. *Let $\mathcal{E} = (G, E, D)$ be a public key encryption scheme defined over $(\mathcal{M}, \mathcal{C})$, and let A be an efficient adversary. We define A's* ***semantic security advantage*** *as:*

$$Adv_{SS}[A, \mathcal{E}] := Pr[Exp_{A,\mathcal{E}}(1) = 1] - Pr[Exp_{A,\mathcal{E}}(0) = 1]$$

4.3 Semantic Security

Definition 5. *A public key encryption scheme $\mathcal{E}$ is* ***semantically secure*** *if for all efficient adversaries A:*

$$Adv_{SS}[A, \mathcal{E}] < \epsilon$$

5 Trapdoors

Definition 6. *Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets. A* ***trapdoor function scheme*** *$\mathcal{T}$, defined over $(\mathcal{X}, \mathcal{Y})$ is a triple of efficient algorithms: (G, F, I):*

1. *$G()$: a randomized algorithm that outputs a key pair (pk, sk)*

2. *$F(pk, \cdot)$: a deterministic algorithm that defines a function $\mathcal{X} \to \mathcal{Y}$*

3. *$I(sk, \cdot)$: a function $\mathcal{Y} \to \mathcal{X}$ that inverts $F(pk, \cdot)$. (This is the "trapdoor".)*

The ***correctness property*** *should be satisfied: for all possible outputs (pk, sk) of G, and for all $x \in \mathcal{X}$, we have $I(sk, F(pk, x)) = x$.*

If $F(pk, \cdot)$ is a permutation on $\mathcal{X}$, we can call $\mathcal{E}$ a **trapdoor permutation scheme**.

5.1 One-way Trapdoor Adversarial Game

Definition 7. *Let $\mathcal{T} = (G, F, I)$ be a trapdoor function scheme defined over $(\mathcal{X}, \mathcal{Y})$. The one-way trapdoor game is defined as follows:*

1. *The Challenger computes $(pk, sk) \leftarrow G()$, samples $x \in \mathcal{X}$ uniformly at random, and then computes $y \leftarrow F(pk, x)$*

2. *The Challenger sends (pk, y) to the Adversary.*

3. *The Adversary outputs $x' \in \mathcal{X}$.*

5.2 One-way Trapdoor Advantage

Let $\mathcal{T} = (G, F, I)$ be a trapdoor function scheme defined over $(\mathcal{X}, \mathcal{Y})$, and let A be an adversary. We define A's **one-way trapdoor advantage** as:

$$Adv_{OW}[A, \mathcal{T}] = Pr[x' = x]$$

5.3 One-way Trapdoor

Let $\mathcal{T} = (G, F, I)$ be a trapdoor function scheme defined over $(\mathcal{X}, \mathcal{Y})$. We say that $\mathcal{T}$ is **one-way** if for all adversaries A:

$$Adv_{OW}[A, \mathcal{T}] < \epsilon$$

6 RSA

Definition 8. *RSA is a trapdoor permutation scheme defined as follows:*

1. *$G()$: Choose random primes p, q, and let $N = p \cdot q$. Choose integers e, d such that $e \cdot d \equiv 1 \pmod{()} p - 1)(q - 1)$. Output $(pk = (N, e), sk = (N, d))$*

2. *$F(pk, x) := x^e \mod N$*

3. *$I(sk, y) := y^d \mod N$*

RSA is assumed to be a one-way trapdoor permutation.