Exercise 5 – Introduction to Cryptography 89-656

Due Date: December 30, 2018

December 16, 2018

Exercise 1: Let $(\mathbb{G}, g, q)$ be a group, and assume that the DDH problem is hard in $\mathbb{G}$. Prove that the following holds: For every algorithm PPT D there exists a negligible function negl such that

$$\left|\Pr[D(g, A, A^y, B, B^x, g^{x+y}) = 1] - \Pr[D(g, A, A^y, B, B^x, g^z) = 1]\right| \leq \mathsf{negl}(n)$$

where $A = g^a$, $B = g^b$ and $a, b, x, y, z \leftarrow \mathbb{Z}_q$ are random.

Exercise 2: Prove formally that if the DDH problem is hard, then so is the CDH problem. Prove formally that if the CDH problem is hard then so is the DLOG problem.

Exercise 3: Consider the following key-exchange protocol:

1. Alice chooses $k, r \leftarrow \{0,1\}^n$ at random, and sends $s := k \oplus r$ to Bob.
2. Bob chooses $t \leftarrow \{0,1\}^n$ at random and sends $u := s \oplus t$ to Alice.
3. Alice computes $w := u \oplus r$ and sends w to Bob.
4. Alice outputs k and Bob computes $w \oplus t$.

Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e., either prove its security or show a concrete attack).

Exercise 4: Show formally that if $\mathcal{P} = \mathcal{NP}$ then there does not exist a CPA-secure public-key encryption scheme.

Exercise 5: Consider the following variant of El Gamal encryption. Let $p = 2q + 1$, let $\mathbb{G}$ be the group of squares modulo p (so $\mathbb{G}$ is a subgroup of $\mathbb{Z}_p^*$ of order q), and let g be a generator of $\mathbb{G}$. The private key is $(\mathbb{G}, g, q, x)$ and the public key is $(\mathbb{G}, g, q, h)$, where $h = g^x$ and $x \in \mathbb{Z}_q$ is chosen uniformly. To encrypt a message $m \in \mathbb{Z}_p$, choose a uniform $r \in \mathbb{Z}_q$, compute $c_1 := g^r \bmod p$ and $c_2 := h^r + m \bmod p$, and let the ciphertext be $\langle c_1, c_2 \rangle$. Is this scheme CPA-secure? Prove your answer.

Exercise 6: Let $\mathbb{G}$ be a cyclic group of order q and let g be the generator. Denote an ElGamal public key by h.

1. Assume that you are given the ElGamal public key and a ciphertext (u, v) encrypting an unknown message $m \in \mathbb{G}$. Show how you can generate a new ciphertext (u', v') that encrypts the same m, but where u' is distributed uniformly in $\mathbb{G}$ (and independently of u).

2. Assume that you are given two ElGamal ciphertexts (u_1, v_1) and (u_2, v_2), encrypting unknown messages m_1 and m_2. Show how to generate a valid encryption of $m_1 \cdot m_2$?

3. Consider a variant of ElGamal where encryption is defined by $(u, v) = (g^r, h^r \cdot g^m)$, where $r \leftarrow \mathbb{Z}_q$ is randomly chosen. For this variant:

   (a) Assume that you are given two ElGamal ciphertexts (u_1, v_1) and (u_2, v_2), encrypting unknown messages m_1 and m_2. Show how to generate a valid encryption of $m_1 + m_2$?

   (b) Is this variant of ElGamal a valid encryption scheme for messages in the domain $\mathbb{Z}_q$?

   (c) Assume that this variant is used for encrypting messages in a small domain (e.g., of polynomial size). Show how decryption can be carried out. Prove that this scheme is CPA-secure.

Exercise 7: Consider the following proposal for probabilistic RSA. Let (N, e) be the public key and let (N, d) be the private key. Let $m \in \mathbb{Z}_N^*$ be the message to be encrypted:

1. A random $r \leftarrow \mathbb{Z}_N^*$ is chosen

2. Compute $c_1 = r^e \bmod N$

3. Compute $c_2 = r + m^e \bmod N$

4. Output (c_1, c_2)

Show how to decrypt. Analyze the security of the scheme under chosen-plaintext and chosen-ciphertext attacks; prove your answers where possible.