Problem Set 11

We will work on the following exercises together during the work sessions on Tuesday, 17 October 2017.

You are strongly encouraged to work together on the exercises, including the homework. You do not have to hand in solutions to these problem sets.

Problem 1: Exercise 11.1 in [KL]: Perfectly secure public key encryption?

Assume a public-key encryption scheme for single-bit messages with no decryption error. Show that, given pk and a ciphertext c computed via $c = \mathrm{Enc}_p k(m)$, it is possible for an unbounded adversary to determine m with probability 1.

Problem 2: Exercise 11.6 in [KL]: El Gamal variant.

Consider the following public-key encryption scheme. The public key is (G, q, g, h) and the private key is x, generated exactly as in the El Gamal encryption scheme. In order to encrypt a bit b, the sender does the following:

1. If $b = 0$ then choose a random $y \leftarrow \mathbb{Z}_q$ and compute $c_1 = g^y$ and $c_2 = h^y$. The ciphertext is (c_1, c_2).

2. If $b = 1$ then choose independent random $y, z \leftarrow \mathbb{Z}_q$, compute $c_1 = g^y$ and $c_2 = g^z$, and set the ciphertext equal to (c_1, c_2).

Show that it is possible to decrypt efficiently given knowledge of x. Prove that this encryption scheme is CPA-secure if the decisional Diffie-Hellman problem is hard relative to $\mathcal{G}$.

Problem 3: Exercise 11.5 in [KL].

Show that Claim 11.7 does not hold in the setting of CCA-security. Exhibit a concrete attack on a scheme $\Pi' = (\mathrm{Gen}, \mathrm{Enc}', \mathrm{Dec}')$ constructed from a fixed lenght CCA secure encryption scheme $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ by defining $\mathrm{Enc}'_k(m_1 \| m_2 \| ... \| m_l) = \mathrm{Enc}_k(m_1) \| \mathrm{Enc}_k(m_2) \| ... \| \mathrm{Enc}_k(m_l)$.

Problem 4: PKCS #1 v1.5

Describe one reason why a proof of CPA security of PKCS #1 v1.5 based on the RSA assumption alone has to fail.