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: El Gamal encryption

As in Example 11.17 in [KL], let $\mathbb{G}$ be the subgroup of $\mathbb{Z}_{167}^*$ generated by $g = 4$. We have that the order $q = |\mathbb{G}| = 83$ is prime. Let the secret key be $x = 23 \in \mathbb{Z}_{83}$ and so the public key is $pk = \langle p, q, g, h\rangle = \langle p, q, g, g^x\rangle$

(a) Compute the h component in the public key.

(b) Compute the encryption of message $m = 19 \in \mathbb{G}$ with randomness $y = 44$.

(c) Decrypt the ciphertext $\langle c_1, c_2\rangle = \langle 132, 44\rangle$.

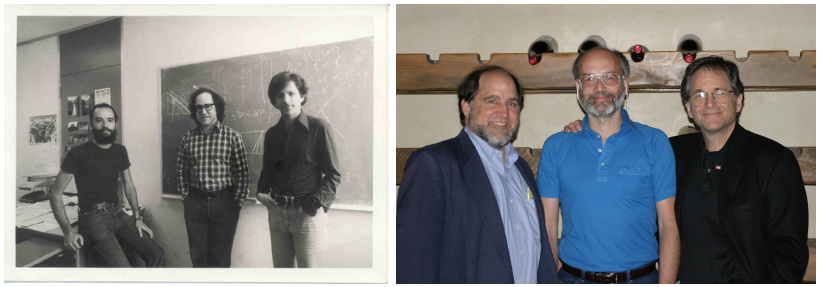
Problem 2: RSA encryption

As in Example 11.27 in [KL], say GenRSA outputs $(N, e, d) = (1005973, 89, d)$. Note that $1005973 = 997 \cdot 1009$.

(a) Encrypt the message $m = 1234 \in \mathbb{Z}_{1005973}^*$

(b) Compute the private key (N, d) corresponding to the public key $(N, e) = (1005973, 89)$.

(c) Decrypt the ciphertext $c = 530339$.



Adi Shamir, Ron Rivest, and Len Adleman as MIT-students and in 2003
Image credit:
http://www.ams.org/samplings/feature-column/fcarc-internet,
http://www.usc.edu/dept/molecular-science/RSA-2003.htm.

Problem 3: Attacks on Plain RSA

(a) For the RSA public key $(N, e) = (10000799791, 3)$, decrypt the ciphertext $c = 1000000$. Can you do it without factoring N?

(b) Suppose we would like to use plain RSA as public-key encryption in a hybrid scheme together with AES-256 in CBC mode. We choose N to have roughly 2048 bits. Use the previous subexercise to argue the insecurity of this hybrid scheme.

Problem 4: 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 $c = \mathsf{Enc}_{pk}(m)$, it is possible for an unbounded adversary to determine m with probability 1.

Problem 5: CCA security of multiple encryptions

Claim 11.7 in [KL] states that if $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a CPA-secure public-key encryption scheme for fixed-length messages, then the new encryption scheme $\Pi' = (\mathsf{Gen}, \mathsf{Enc}', \mathsf{Dec}')$ with $\mathsf{Enc}'_{pk}(m_1\|m_2\|...\|m_\ell) = \mathsf{Enc}_{pk}(m_1)\|\mathsf{Enc}_{pk}(m_2)\|...\|\mathsf{Enc}_{pk}(m_\ell)$ is CPA secure for arbitrary-length messages.

Show that Claim 11.7 does not hold in the setting of CCA-security: Exhibit a concrete attack on a scheme $\Pi' = (\mathsf{Gen}, \mathsf{Enc}', \mathsf{Dec}')$ constructed from a fixed-length CCA secure encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ by defining

$$\mathsf{Enc}'_{pk}(m_1\|m_2\|...\|m_\ell) = \mathsf{Enc}_{pk}(m_1)\|\mathsf{Enc}_{pk}(m_2)\|...\|\mathsf{Enc}_{pk}(m_\ell)$$

★

Problem 6: 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 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).
2. If $b = 1$ 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).

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 $\mathcal{G}$.