Introduction to Modern Cryptography
Exercise Sheet #6

University of Amsterdam, Master of Logic, 2014
Lecturer: Christian Schaffner
TA: Malvin Gattinger

Monday, 6 October 2014
(to be handed in by Monday, 13 October 2014, 11:00)

Homework

1. **Impossibility of perfectly-secure public-key encryption:** Exercise 10.1 in [KL]: Assume a public-key encryption scheme for single-bit messages. Show that, given pk and a ciphertext c computed via $c \leftarrow \mathsf{Enc}_{pk}(m)$, it is possible for an unbounded adversary to determine m with probability 1. This shows that perfectly-secret public-key encryption is impossible. 10 p.

2. **Hybrid Encryption** 20 p.

   (a) **Computational Indistinguishability:** Show that computational indistinguishability of probability ensembles (as defined in Definition 6.34 of [KL]) is transitive. Show that if both $X \overset{c}{\equiv} Y$ and $Y \overset{c}{\equiv} Z$ hold, we also have $X \overset{c}{\equiv} Z$.

   (b) **Reduction:** Using the notation from the lecture, show that

   $$(pk, \mathsf{Enc}_{pk}(k), \widetilde{\mathsf{Enc}}_k(m_0)) \overset{c}{\equiv} (pk, \mathsf{Enc}_{pk}(0^n), \widetilde{\mathsf{Enc}}_k(m_0))$$

   Consider a distinguisher $\mathcal{D}$ which distinguishes the above ensembles with probability $\varepsilon_{\mathcal{D}}(n)$, i.e.

   $$\varepsilon_{\mathcal{D}}(n) = \left| \Pr[\mathcal{D}(pk, \mathsf{Enc}_{pk}(k), \widetilde{\mathsf{Enc}}_k(m_0)) = 1] - \Pr[\mathcal{D}(pk, \mathsf{Enc}_{pk}(0^n), \widetilde{\mathsf{Enc}}_k(m_0)) = 1] \right| .$$

   In order to show that $\varepsilon_{\mathcal{D}}(n) \leq \mathsf{negl}(n)$, construct a CPA-attacker $\mathcal{A}$ on Π which uses $\mathcal{D}$ as a subroutine. **Hint**: Look at the proof of Theorem 10.13 in [KL]. Note that the solution must be in your own words.

3. **Factoring RSA Moduli:** Let $N = pq$ be a RSA-modulus and let $(N, e, d) \leftarrow \mathsf{GenRSA}$. In this exercise, you show that for the special case of $e = 3$, computing d is equivalent to factoring N. Show the following: 20 p.

   (a) The ability of efficiently factoring N allows to compute d efficiently. This shows one implication.

   (b) Given $\phi(N)$ and N, show how to compute p and q. **Hint:** Derive a quadratic equation (over the integers) in the unknown p.

   (c) Assume we know $e = 3$ and $d \in \{1, 2, \ldots, \phi(N) - 1\}$ such that $ed \equiv 1 \mod \phi(N)$. Show how to efficiently compute p and q. **Hint:** Obtain a small list of possibilities for $\phi(N)$ and use (b).

   (d) Given $e = 3$, $d = 29'531$ and $N = 44'719$, factor N using the method above.

4. **RSA-Padding and CCA-Security:** Exercise 10.14 in [KL]: Consider the following version of padded RSA encryption. Assume that the message m to be encrypted has length $\|N\|/2$. To encrypt, first pad m to the left with one byte of zeroes, then 10 random bytes, and then all zeroes; the result is denoted $\bar{m}$ (that is, $\bar{m} = (0^k \| r \| 00000000 \| m)$, where k is the number of zeroes needed 10 p.

to make $\bar{m}$ the appropriate size). Finally, compute $c = [\bar{m}^e \mod N]$. Describe a chosen-ciphertext attack on this scheme. Why is it easier to construct a chosen-ciphertext attack on this scheme than on PKCS #1 v1.5?

Hint: Use messages m_0, m_1 whose ciphertexts you can transform into different valid ciphertexts if the most significant bit of the random part r of the padding is 0.

5. **El Gamal Variant:** Exercise 10.11 in [KL]: 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 Elgamal encryption scheme. In order to encrypt a bit b, the sender does the following: 15 p.

   (a) 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).

   (b) 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 $\mathcal{G}$.

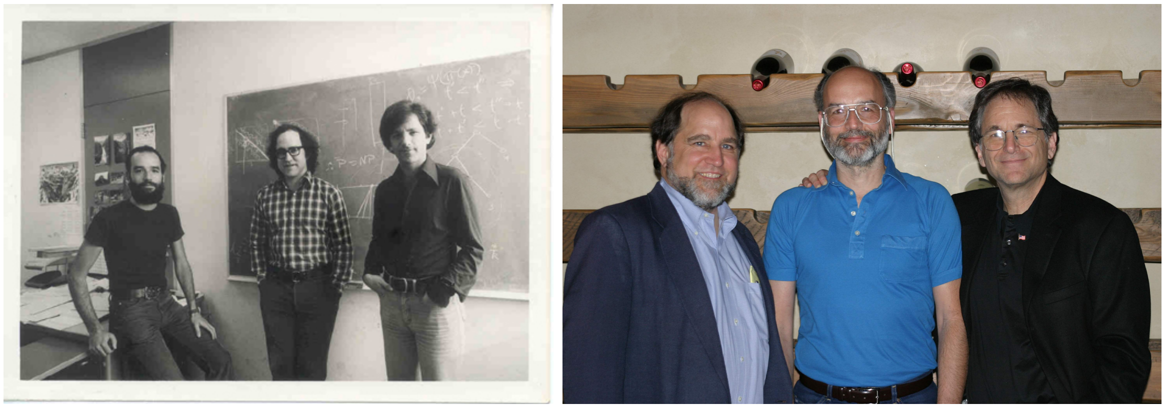
6. **Secure Coin-Flipping:** Exercise 10.17 in [KL]: Consider the following protocol for two parties A and B to flip a fair coin (more complicated versions of this might be used for Internet gambling): 15 p.

   1. A trusted party T publishes her public key pk;
   2. A chooses a random bit b_A, encrypts it using pk, and announces the ciphertext c_A to B and T;
   3. B acts symmetrically and announces a ciphertext $c_B \neq c_A$;
   4. T decrypts both c_A and c_B, and the parties XOR the results to obtain the value of the coin.

   (a) Argue that even if A is dishonest (but B is honest), the final value of the coin is uniformly distributed.

   (b) Assume the parties use Elgamal encryption (where the bit b is encoded as the group element g^b). Show how a dishonest B can bias the coin to any value he likes.

   (c) Suggest what type of encryption scheme would be appropriate to use here. Can you define an appropriate notion of security and prove that your suggestion achieves this definition?



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`.