Skriftlig Eksamen
Kryptologi

Institut for Matematik og Datalogi
Syddansk Universitet - Odense Universitet

Tirsdag den 19. juni 2000, kl. 9–13

Alle sædvanlige hjælpemidler (lærebøger, notater, etc.) samt brug af lommeregner er tilladt.

Eksamenssættet består af 4 opgaver på 4 nummererede sider (1–4). Fuld besvarelse er besvarelse af alle 4 opgaver. Opgavernes vægt ved bedømmelsen er angivet i parenteser ved starten af hver opgave.

Der må gerne refereres til algoritmer og resultater fra lærebogen inklusive øvelsesopgaverne. Specielt må man gerne begrunde en påstand med at henvise til, at det umiddelbart følger fra et resultat i lærebogen (hvis dette altså er sandt!). Henvisninger til andre bøger (udover lærebogen) accepteres ikke som besvarelse af et spørgsmål.

Bemærk, at hvis der er et spørgsmål i en opgave, man ikke kan besvare, kan man godt besvare de efterfølgende spørgsmål og blot antage at man har en løsning til de foregående spørgsmål.

Problem 1 (20%)

a. In the ElGamal Public-key Cryptosystem in Z_p^*, the user doing the encryption chooses a random secret value $k \in Z_{p-1}$. Suppose that user encrypts a message m using a particular value k' for this k, and k' is not kept secret. How could a cryptanalyst use k' to find m?

b. In the Menezes-Vanstone Elliptic Curve Cryptosystem, the user doing encryption chooses a random secret value $k \in Z_{|H|}$. Suppose that user encrypts a message m using a particular value k' for this k, and k' is not kept secret. How could a cryptanalyst use k' to find m?

c. Explain why it is recommended that a one-time pad not be used more than once.

d. The known-plaintext attack on the linear feedback shift register stream cipher discussed in the textbook requires n bits of plaintext and n corresponding bits of cipher text where $n = 2m$ (and the recurrence has degree m) to reconstruct the entire key stream. Suppose that instead of $2m$ bits of plaintext and corresponding ciphertext, the cryptanalyst has only $2m - 2$ bits. How would this cryptanalyst reconstruct the entire key stream?

Problem 2 15%

Given an RSA modulus n, a ciphertext c, and the encryption exponent e, we know that $c \equiv m^e \pmod{n}$ for some secret message m. One method of trying to find m is to perform a so-called *cycling attack*, which is rather similar to Pollard's rho method for factoring. One can construct the sequence defined inductively by $x_0 = c$ and $x_{i+1} \equiv x_i^e \pmod{n}$ for $i \geq 0$. If at some point one finds x_{i+1} such that $\gcd(x_{i+1} - x_0, n) \neq 1$, there is enough information to find the message m. There are two cases to consider:

- Case 1: $\gcd(x_{i+1} - x_0, n) = n$.
- Case 2: $\gcd(x_{i+1} - x_0, n) < n$.

a. Explain how m can be found from x_i in Case 1.

b. Explain how m can be found in Case 2.

c. Suppose that RSA is secure with the modulus n. What would you expect to be the average length of this sequence a cryptanalyst would have to produce before finding a "good" x_{i+1}? You do not need to be precise.

Problem 3 (30%)

Let g, h, and f be elements of the group Z_p^*, where p is prime. To show that f is in the subgroup generated by the two elements g and h, one can execute the following protocol $\lceil \log_2 p \rceil$ times. Suppose that p, g, h, and f are given as input to a Prover and Verifier. Assume the Prover knows an x and a y such that $f \equiv g^x h^y \pmod{p}$.

Prover		Verifier
Choose random $k, l \in \{1, ..., p-1\}$. Let $z = f \cdot g^k \cdot h^l \pmod{p}$.	$\xrightarrow{\quad z \quad}$	
		Choose a random $b \in \{0, 1\}$.
	$\xleftarrow{\quad b \quad}$	
Let $r_1 = k + b \cdot x \pmod{p-1}$, and $r_2 = l + b \cdot y \pmod{p-1}$.	$\xrightarrow{(r_1, r_2)}$	
		Check that , $z = f^{1-b} \cdot g^{r_1} h^{r_2} \pmod{p}$. If not, reject and halt.

a. Prove that the above protocol is an interactive proof system showing that $f \equiv g^{x'} \cdot h^{y'} \pmod{p}$ for some integers x' and y'.

b. Suppose that $f \equiv g^{x'} \cdot h^{y'} \pmod{p}$ for some integers x' and y'. What is the probability distribution of the values (z, r_1, r_2) sent by a Prover following the protocol?

c. Prove that the above protocol is perfect zero-knowledge (use definition 13.2 in the textbook).

Problem 4 (35%)

Suppose that p is a prime. The element g is a generator of the group Z_p^* if and only if for every $h \in Z_p^*$ there is an x such that $g^x \equiv h \pmod{p}$.

a. Suppose we choose an element h uniformly at random in Z_p^*. Show that if g is not a generator of Z_p^*, then the probability that there exists x such that $h \equiv g^x \pmod{p}$ is at most $1/2$.

b. Give a zero-knowledge proof that g is a generator for Z_p^*. Show that it is an interactive proof system. Show that it is zero-knowledge.

c. Can your protocol be executed by an efficient (polynomial time) prover? Why or why not?