CS 519
Cryptography and Network Security
Instructor: Ali Aydın Selçuk
Department of Computer Engineering, Bilkent University

Midterm Exam

November 5, 2003

Question 1. (*40 pts.*) Answer briefly (i.e., in no more than 4-5 lines) each of the following questions:

a. In his book "The Road Ahead", Bill Gates writes that the security of RSA is based on the "difficulty of factoring large primes". Is the problem of factoring large primes really difficult?

b. What is the significance of the key schedule in modern block ciphers? (I.e., can't these ciphers be designed without a key schedule?)

c. Is a fixed or a random IV preferable in a CBC-MAC computation? Why?

d. What is the mechanism for providing diffusion in Rijndael? Briefly explain the diffusion-related operations and their roles.

e. If DES encryption is performed in the OFB mode with a weak DES key, what pseudo-random stream will be generated?

f. As MACs can be produced from hash functions, consider producing a hash function from CBC-MAC, where the CBC checksum of a message is computed using a fixed key and IV. Would this hash function be secure? Why/why not?

g. What is the "broadcast with a common exponent" problem in RSA? How does the PKCS solve it?

h. A dishonest dealer might distribute "bad" shares for a Shamir threshold scheme, i.e., shares for which different t-subsets determine different keys. Given all n shares, we could test the consistency of the shares by computing the key for every one of the $\binom{n}{t}$ t-subsets of participants, and verifying that the same key is computed in each case. Describe a more efficient method for testing the consistency of the shares.

Turn the page

Question 2. (*20 pts.*) Recall from the DESX construction that for a block cipher F with an n-bit key and ℓ-bit block size, FX is defined by

$$FX_{k,k_1,k_2}(x) = F_k(x \oplus k_1) \oplus k_2$$

where $k \in \{0,1\}^n$, $k_1, k_2 \in \{0,1\}^\ell$.

Show that the simplified constructions

$$\begin{aligned} FY_{k,k_1}(x) &= F_k(x \oplus k_1) \\ FZ_{k,k_1}(x) &= F_k(x) \oplus k_1 \end{aligned}$$

do not increase the strength of the cipher against exhaustive search. That is, show that FY and FZ each can be broken using in the order of 2^n operations. (You can assume that a moderate number of known plaintext-ciphertext blocks are available for your attacks.)

Question 3. (*20 pts.*) Alice and Bob use AES CBC-MAC with a shared key to authenticate their communications. To prevent variable-length message attacks, they append the number of blocks to the message as a separate block before computing the CBC-MAC. That is,

$$\text{MAC}(M) = \text{CBC-MAC}(M \| n)$$

where n is the number of blocks in M.

Eve wants to send a certain message to Bob, making it appear to be from Alice. The message M consists of n blocks, $M_1 M_2 \ldots M_n$, where the $(n-1)$st block M_{n-1} can be anything, but all other blocks must have a certain content. Show how Eve can forge a valid MAC for M by an adaptive chosen-message attack.

Question 4. (*20 pts.*) In an RSA-based secure communications system, it may be desirable to simplify the key generation and management process by using a system-wide common modulus N, generated by a trusted key generation authority, and user-specific key pairs (e, d). Show that such a common-modulus system is totally insecure against insider attacks by proving the following steps:

a. Eve, possessing a key pair (e_E, d_E), can easily compute a multiple of $\phi(N)$, say $k \cdot \phi(N)$.

b. If Alice's public key e_A is relatively prime to k, Eve can find a decryption exponent for Alice and read all her messages.

c. Eve can compute a decryption exponent for any user in the system, whether or not $\gcd(e, k) = 1$.

Good luck