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

---

# Midterm Exam

November 11, 2005

**Question 1.** (*40 pts.*) Answer briefly each of the following questions:

a. Why is an extra swap between the left and right half-blocks desired in the last round of a Feistel cipher?

b. Would CFB-MAC—with the last output block of the CFB computation over a data packet appended to the packet as a checksum—be a secure MAC? Why/why not?

c. Consider modifying the MAC scheme in 802.11 such that the CRC checksum is encrypted with a block cipher (say, AES) while the message is still encrypted with RC4. Would an attack like the current ciphertext modification attack work? Why/why not?

d. Does collision-resistance imply one-wayness? Explain briefly.

e. What is the "guessable plaintext" problem in public key encryption? Is it a problem for ElGamal encryption as well? Why/why not?

f. Can the Merkle-Hellman knapsack cryptosystem be used as a signature algorithm in a straightforward manner—using the private key operation for signing and the public key operation for verification? Why/why not? (Assume the input is always hashed before signing; hence existential forgery attacks are not applicable.)

g. Why the same $k$ value should not be used multiple times in ElGamal encryption?

h. What is the basic idea of ID-based encryption? Explain briefly.

*Turn the page*

**Question 2.** (*20 pts.*) Recall from the DESX construction that for a block cipher $F$ with an $n$-bit key and $\ell$-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.*) A misuse of the ElGamal signature scheme is to use the same $k$ value multiple times. Show that if Bob signs two different messages $m_1$, $m_2$ with the same $k$ value and obtains the signatures $(r, s_1)$, $(r, s_2)$, Trudy can produce a valid signature for any message she likes. (Hint: First work by assuming $\gcd(s_1 - s_2, p-1) = 1$—or, equivalently, $\gcd(m_1 - m_2, p-1) = 1$. Then generalize your proof to arbitrary $s_1$, $s_2$.)

**Question 4.** (*20 pts.*) In a secret sharing system, it may be desirable to update the shares periodically, while keeping the secret unchanged, so that a long-term secret may remain safe over a long period of time. If the dealer is not available after the initial distribution, the update will have to be done by parties who don't know the secret.

a. Consider realizing such a system with Shamir's secret sharing scheme. Describe how the update function can be achieved. (I.e., in an $(n,t)$-sharing of a key $k$ where the $i$th party's share is $(i, y_i)$, for $i = 1, 2, \ldots n$, some party distributes "update shares" $u_i$ to party $i$ so that $y_i$ is updated as $y'_i = y_i + u_i \bmod p$. Describe how such update shares can be generated by someone who doesn't know the key such that the resulting system $(i, y'_i)$, for $i = 1, 2, \ldots n$, remains an $(n,t)$-sharing of the key $k$.

b. Since we don't know which parties may get compromised over time, it is desirable that all $n$ parties contribute to the share update protocol. Describe a *simple* generalization of your solution in part (a) where shares are updated periodically by the contribution of all $n$ members. (You can assume that encrypted channels exist between every pair of members so that the update shares can be exchanged securely.)

*Good luck*