Cryptography and Communication Security	**Midterm**
CSG 252 Fall 2006	**Due: 11/16/2006**

Note on integrity: For the midterm, you are not allowed to discuss problems with fellow students. All written work must be entirely your own, and cannot be from any other course.

Questions

(1) Let P be a 6-digit number in the range $[0, 10^6 - 1]$ encrypted with a shift cipher with key K, $0 \leq K \leq 9$. For example, if $K = 1$, $P = 123456$ is encrypted as 234567. Compute $H(P)$, $H(C)$, $H(K)$, $H(P \mid C)$, $H(K \mid C)$, assuming all values of P and K are equivally likely.

(2) Recall the following algorithm to compute the round keys k_i, $i = 1, \ldots, 16$ for DES from the 64-bit key k. Only 56 of the 64 bits are used and permutated. This is done by a map *PC1*. The result $PC1(k)$ is divided into two halves, C_0 and D_0, of 28 bits.

$$
\begin{array}{l}
\textit{bitString DESKeyGenerator } (\textit{bitString } k) \\
\quad (C_0, D_0) \leftarrow PC1(k) \\
\quad \textit{for } i \leftarrow 1 \textit{ to } 16 \textit{ do} \\
\quad\quad (C_i, D_i) \leftarrow (LS_i(C_{i-1}), LS_i(D_{i-1})) \\
\quad\quad k_i \leftarrow PC2(C_i, D_i) \\
\quad \textit{return } k_1, \ldots, k_{16}
\end{array}
$$

Here LS_i is a cyclic left shift by one position if $i = 1, 2, 9, 16$, and by two positiions otherwise. The maps $PC_1 : \{0,1\}^{64} \to \{0,1\}^{56}$ and $PC_2 : \{0,1\}^{56} \to \{0,1\}^{48}$ are defined by the tables:

$$57, 49, 41, 33, 25, 17, 9, 1, 58, 50, 42, 34, 26, 18, 10, 2, 59, 51, 43, 35, 27, 19, 11,$$
$$3, 60, 52, 44, 36, 63, 55, 47, 39, 31, 23, 15, 7, 62, 54, 46, 38, 30, 22, 14, 6, 61, 53,$$
$$45, 37, 29, 21, 13, 5, 28, 20, 12, 4$$

and

$$14, 17, 11, 24, 1, 5, 3, 28, 15, 6, 21, 10, 23, 19, 12, 4, 26, 8, 16, 7, 27, 20, 13, 2,$$
$$41, 52, 31, 37, 47, 55, 30, 40, 51, 45, 33, 48, 44, 49, 39, 56, 34, 53, 46, 42, 50,$$
$$36, 29, 32$$

The tables are read line by line and describe how to get the images, i.e., $PC_1(x_1, \ldots, x_{64}) = (x_{57}, x_{49}, \ldots, x_{12}, x_4)$ and $PC_2(x_1, \ldots, x_{56}) = (x_{14}, x_{17}, \ldots, x_{29}, x_{32})$.

The bits $8, 16, 24, 32, 40, 48, 56, 64$ of k are not used. They are defined in such a way that odd parity holds for each byte of k. A key k is defined to be *weak* if $k_1 = k_2 = \cdots = k_{16}$.

Show that exactly four weak keys exist, and determine these keys.

(3) Set up an ElGamal encryption scheme by generating a pair of public and secret keys.

(a) Choose a suitable plaintext and ciphertext. Encrypt and decrypt them.

(b) Generate ElGamal signatures for suitable messages. Verify the signatures.

(c) Forge a signature without using the secret key.

(d) Play the role of an adversary Eve, who learns the random number k used to generate a signature, and break the system.

(e) Demonstrate that checking the condition $1 \leq r \leq p - 1$ is necessary in the verification of a signature (r, s).