T-79.5501 Cryptology
Homework 1
January 23, 2007

1. Discuss the following claims. Which of them are true and which are just generally believed to be true?

   a) If RSA with modulus n is secure, then factoring of n is hard.

   b) If the *Discrete Logarithm Problem* in group G is hard, then the Diffie-Hellman key exchange in G is secure.

   c) If Diffie-Hellman key exchange in group G is secure, then the *Discrete Logarithm Problem* in group G is hard.

   d) Given one plaintext-ciphertext pair, computational effort of finding a 128-bit key used in the AES is at least 2^{100} operations.

2. Let us consider a cryptosystem where $\mathcal{P} = \{a, b, c\}$ and $\mathcal{C} = \{1, 2, 3, 4\}$, $\mathcal{K} = \{K_1, K_2, K_3\}$, and the encryption mappings e_K are defined as follows:

K	$e_K(a)$	$e_K(b)$	$e_K(c)$
K_1	1	2	3
K_2	2	3	4
K_3	3	4	1

   Given that keys are chosen equiprobably, and the plaintext probability distribution is $\mathbf{Pr}[a] = 1/2$, $\mathbf{Pr}[b] = 1/3$, $\mathbf{Pr}[c] = 1/6$, compute the following probabilities

   a) $\mathbf{Pr}[\mathbf{y} = i]$, $i = 1, 2, 3, 4$.

   b) $\mathbf{Pr}[\mathbf{x} = j, \mathbf{y} = i]$, $j = a, b, c$, and $i = 1, 2, 3, 4$..

3. Plaintext is composed of independently generated bits that are arranged in blocks of four bits. The probability that a plaintext bit equals 0 is p. Each block x_1, x_2, x_3, x_4 is encrypted using one key bit z by adding it modulo 2 to each plaintext bit. Hence the ciphertext block is y_1, y_2, y_3, y_4 where $y_i = x_i \oplus z$, $i = 1, 2, 3, 4$. It is assumed that every key bit is generated uniformly at random. Let us assume that a ciphertext block has k zeroes and $4 - k$ ones, $k = 0, 1, 2, 3, 4$.

   a) Compute the probability (as a funcion of k) that the encryption key was $z = 0$.

   b) What value of k maximizes this probability?

   c) For which value of k the probability that $z = 0$ is equal to $\frac{1}{2}$, that is, the ciphertext does not give any information at all about the used key bit?

4. The **Affine Cipher** is a cryptosystem with $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ and $\mathcal{K} = \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}$. The set $\mathbb{Z}_{26}^*$ consists of the numbers a with $\gcd(a, 26) = 1$. The encryption rule is defined as

$$e_K(x) = ax + b \bmod 26, \text{ for } x \in \mathcal{P}, \text{ where } (a, b) \in \mathcal{K}.$$

   a) Determine the decryption rule d_K.

   b) Prove that the **Affine Cipher** achieves perfect secrecy.

5. Consider a cryptosystem where $\mathcal{P} = \{A, B\}$ and $\mathcal{C} = \{a, b, c\}$, $\mathcal{K} = \{1, 2, 3, 4\}$, and the encryption mappings e_K are defined as follows:

K	$e_K(A)$	$e_K(B)$
1	a	b
2	b	c
3	b	a
4	c	a

The keys are chosen with equal probability.

a) Show that

$$\mathbf{Pr}[\mathbf{x} = A | \mathbf{y} = a] = \frac{\mathbf{Pr}[\mathbf{x} = A]}{2 - \mathbf{Pr}[\mathbf{x} = A]}.$$

b) Does this cryptosystem achieve perfect secrecy?