Computer and Network Security: Homework 1

Instructions

- Please answer 5 of the 6 problems. All questions are weighted equally.
- Please send your solution to 2160853158@qq.com by Oct. 8 midnight.

Problem 1 Vigenère Cipher. Suppose you have a language with only the 3 letters A, B, C, and they occur with frequencies 0.7, 0.2, and 0.1. The following ciphertext was encrypted by the Vigenère cipher:

$$ABCBABBBAC.$$

Suppose you are told that the key length is 1, 2, or 3. Show that the key length is probably 2, and determine the most probable key.

Problem 2 Perfect secrecy and one-time-pad.

1. For a perfect secret encryption scheme $E(K, M) = C$, prove: $\Pr[C = c|M = m] = \Pr[C = c]$.
2. Consider a biased one-time-pad system, where $\Pr[M = b] = p_b$, $b = 0, 1$ and $\Pr[K = 0] = 0.4$. The first attacker Randy randomly guesses $M = 1$ or $M = 1$: prove that the probability of success is 0.5. The second attacker Smarty guesses M based on C and p_0, p_0: suggest a good attack strategy.

Problem 3 DES. Before 2-DES and 3-DES was invented, the researchers at RSA Labs came up with DESV and DESW, defined by

$$DESV_{kk_1}(M) = DES_k(M) \oplus k_1, \; DESW_{kk_1}(M) = DES_k(M \oplus k_1).$$

In both schemes, $|k| = 56$ and $|k_1| = 64$. Show that both these proposals do not increase the work needed to break them using brute-force key search. That is, show how to break these schemes using on the order of 2^{56} DES operations. You have a small number of plaintext-ciphertext pairs.

Problem 4 RSA. Alice and Bob love each other, so they decide to use a single RSA modulus N for their key pairs. Of course each of them does not know the private key of the other. Mathematically, Alice and Bob have their own key pairs (e_A, d_B) and (e_B, d_B) sharing the same N. Demonstrate how Bob can derive the private key of Alice.

Problem 5 Operation mode of block ciphers. Chloé invents a new operation mode as below that can support parallel encryption. Unfortunately, this mode is not secure. Please demonstrate how an attacker knowing IV, C_0, C_1, C_2, and $M_1 = M_2 = M$ can recover M_0.

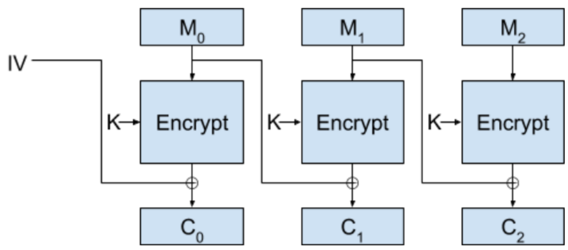

Figure 1: Chloé's invention

Problem 6 Hash functions. One-wayness and collision-resistance are two indispensable properties of hash functions. They are in fact independent one to the other.

1. Give a function that is one-way, but not collision-resistant.
2. Give a function that is collision-resistant, but not one-way.