IIIT Vadodara

CS304: Introduction to Cryptography and Network Security

Midsem **Marks: 30**

Course Instructor: Dr. Dibyendu Roy Time Limit: 120 minutes

Instructions: Question paper is of **2 pages**. Clearly write your name and roll number. Solutions must be written clearly.

(Q1) **[5 marks]**

Describe an efficient algorithm for finding a collision for any hash function $h : X \to Y$, where $|Y| = m$. Derive the success probability of your algorithm. Using this prove that if you take just 23 students from your batch then two among the 23 selected students will share same birthday with $\frac{1}{2}$ probability.

(Q2) **[3 marks]**

Suppose triple DES is performed by choosing two keys K_1, K_2 and computing $E_{K_1}(E_{K_2}(E_{K_2}(m)))$. Show how to attack this modified version with a meet-in-the-middle attack.

(Q3) **[5 marks]**

Suppose E^1 and E^2 are two encryption methods. Let K_1 and K_2 be keys and consider the double encryption

$$E_{K_1,K_2}(m) = E^1_{K_1}(E^2_{K_2}(m)).$$

1. Suppose you know a plaintext-ciphertext pair. Show how to perform a meet-in-the-middle attack on this double encryption.
2. An affine encryption given by $x \mapsto (\alpha x + \beta) (\mathrm{mod} 26)$ can be regarded as a double encryption, where one encryption is multiplying the plaintext by α and the other is a shift by β. Assume that you have a plaintext and a ciphertext that are long enough that α and β are unique. Show that meet-in-the-middle attack from part (a) takes atmost 38 steps (not including the comparisons between the lists). Note that this is much faster than a brute force search through all 312 keys.

(Q4) **[5 marks]**

Consider the following DES-like encryption method. Start with a message of $2n$ bits. Divide it into two blocks of length n (a left half and a right half): M_0M_1. The key K consists of k bits, for some integer k. There is a function $f(K, M)$ that takes an input of k bits and n bits and gives an output of n bits. One round of encryption starts with a pair M_jM_{j+1}. The output is the pair $M_{j+1}M_{j+2}$, where $M_{j+2} = M_j \oplus f(K, M_{j+1})$. This is done for m rounds, so the ciphertext is M_mM_{m+1}.

1. If you have a machine that does the m-round encryption just described, how would you use the same machine to decrypt the ciphertext M_mM_{m+1} (using the same key K)? Prove that your decryption method works.
2. Suppose K has n bits and $f(K, M) = K \oplus M$, and suppose the encryption process consists of $m = 2$ rounds. If you know only a ciphertext, can you deduce the plaintext and the key? If you know a ciphertext and the corresponding plaintext, can you deduce the key? Justify your answers.

(Q5) **[4 marks]**

Define Perfect Secrecy. Suppose the 26 keys in the Shift Cipher are used with equal probability $\frac{1}{26}$. Then prove that for any plaintext probability distribution the Shift Cipher has Perfect Secrecy.

(Q6) **[2 marks]**

Define Ideal Hash function. Prove that $h : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, $h(x, y) = (ax + by) \mod n$ is not an ideal hash function.

(Q7) **[3 marks]**

Compute AES-Subbyte(B5). Input is in hexadecimal.

(Q8) **[3 marks]**

Compute AES-Mixcolumn(154, 212, 93, 201). Input is in decimal.