IIIT Vadodara

CS304: Introduction to Cryptography and Network Security

Endsem **Marks: 45**

Course Instructor: Dr. Dibyendu Roy Time Limit: 180 minutes

Instructions: Question paper is of 2 pages. Clearly write your name and roll number. Answers must be argued properly to get the credit. You can use scientific calculator during the exam.

(Q1) **[9 marks]**

State and prove the Chinese Remainder theorem. Using it find x such that 5

$$x \equiv 5 \mod 37, \quad x \equiv 7 \mod 41, \quad x \equiv 3 \mod 47.$$

(Q2) **[9 marks]**

Describe complete RC4 algorithm. Derive the probability $Pr[Z_2 = 0]$, where Z_2 is the second output from RC4. 8/4

(Q3) **[9 marks]**

Define Discrete Log Problem (DLP) on Elliptic curve EL. Describe an algorithm which can solve the DLP on EL in $O(\sqrt{n})$ complexity where n is the order of the subgroup G_1 generated by the base point P of the Elliptic Curve EL for DLP i.e., $G_1 =< P >$, $|G_1| = n$ and P is the point of EL on which you are defining DLP. 1/2

(Q4) **[9 marks]**

I have made a toy RSA encryption system. I announce to you the public modulus $n = 221$ and the public encryption key $e = 77$. To send an encrypted message m to me (which can be any positive number between 1 and 220), you must calculate $m^{77}($ mod 221). Not content with the ability to send me encrypted messages, you have decided to try to read my encrypted messages. You find that the Dean has sent me the encrypted message 95. What was the Dean's actual message to me? 9

(Q5) **[5 marks]**

Suppose $h_1 : \{0,1\}^{2m} \to \{0,1\}^m$ is a collision resistant hash function. Define $h_2 : \{0,1\}^{4m} \to \{0,1\}^m$ as follows.

(a) Write $x \in \{0,1\}^{4m}$ as $x = x_1||x_2$ where $x_1, x_2 \in \{0,1\}^{2m}$.

(b) Define $h_2(x) = h_1\Big(h_1(x_1)||h_1(x_2)\Big)$.

Prove or disprove the statement "h_2 is collision resistant".

(Q6) **[4 marks]**

Consider the following simplified version of the CFB mode. The plaintext is broken into 32-pieces: $P = [P_1, P_2, \ldots]$, where each P_j has 32-bits, rather than the 8 bits used in CFB. Encryption proceeds as follows. An initial 64-bit X_1 is chosen. Then for $j = 1, 2, 3, \ldots$, the following is performed:

$$C_j = P_j \oplus L_{32}(E_K(X_j))$$

$$X_{j+1} = R_{32}(X_j)||C_j,$$

where $L_{32}(X)$ denotes the 32 leftmost bits of X, $R_{32}(X)$ denotes the rightmost 32 bits of X, and $X||Y$ denotes the bit string obtained by writing X followed by Y.

1. Find the decryption algorithm.
2. The ciphertext consists of 32-bit blocks $C_1, C_2, C_3, \ldots$. Suppose that a transmission error causes C_1 to be received as $\widetilde{C}_1 \neq C_1$, but that $C_2, C_3, C_4 \ldots$ are received correctly. This corrupted ciphertext is then decrypted to yield plaintext blocks $\widetilde{P}_1, P_2, P_3, \ldots$. Show that $\widetilde{P}_1 \neq P_1$, but that $\widetilde{P}_i = P_i$ for all $i \geq 4$. Therefore, the error affects only three blocks of the decryption.