CS 2204-01 Communications and Networking

Instructor: Professor Sharon Sisitzky

Name: Ryohei Hayashi

Learning Journal Unit 8

**Part1**

a. If John sends M2=hash(M1) as a message, it is impossible for Anthony to quickly recover M1. This is because hash functions are one-way functions and it is practically impossible to recover the original message from the hash value.

However, when John later communicates M1 to Anthony, Anthony can confirm that John knew M1 when he sent M2. This is done by chipping the M1 that Anthony received from John into a hash function and checking whether the result matches M2.

b. It is possible to add some information (e.g. a salt or a timestamp) in order to use a secure hash function. For example, John can generate M2 by hashing the message M1 with the addition of a salt. When Anthony performs the verification, John provides both M1 and the salt. Anthony can use the provided M1 and salt to calculate the hash value and compare it with the M2 received from John to confirm that he knew the M1 from the beginning. This allows us to recommend the risk of rainbow table attacks and collision attacks.

**Part2**

1. Two main types of error control mechanisms exist: error detection and error correction.

(a) If the encoded data contains redundant information to recover from errors, the appropriate mechanism is Forward Error Correction (FEC); FEC allows the receiver to detect errors and obtain sufficient information from the redundant data to recover the original data.

(b) If the encoded data contains redundant information that detects corrupted blocks and requires them to be retransmitted, this is classified as an Automatic Retransmission Request (ARQ) mechanism.ARQ is a process that requires the sender to retransmit data when the receiver detects an error.

2. The need to prefix MIME headers when sending web pages is to ensure that the receiving system can correctly identify the type of content and process it appropriately. the MIME header provides important information about the nature of the content being sent, such as the format, encoding, and language of the document It provides important information about the

3. If spam messages are being sent from an employee's computer and the employee does not remember sending the spam himself, the computer may be infected with malware or a virus. This type of attack, where an attacker uses malicious software to take control of a computer, allows spam messages to be sent automatically over a wide area.

4. Voice over IP (VoIP) transmits voice data via the Internet Protocol. Using the User Datagram Protocol (UDP) in this process, data is often sent more quickly, but datagrams (a type of data packet) can be lost or reordered, as UDP does not guarantee the arrival of the transmitted data.

If UDP datagrams arrive out of order, the quality of the voice call may be affected. Specifically, the following problems may occur

Speech fragmentation: if speech data does not arrive in the correct order, the conversation may sound fragmented and difficult to understand.

Jitter: irregular arrival times of datagrams can result in uneven speech reproduction, making it difficult to listen to. This is known as jitter and is one of the main factors reducing the quality of communication.

Increased latency: if the datagrams sent need to be reconstructed in the proper order, the process takes time and may cause delays in the call.

Word-Count: 550