Homework 4

Problem1.

a) What is the security hole of authentication protocol 5.0? How to address this security issue?
b) What characteristics are needed in a secure hash function?
c) What is the role of a compression function in a hash function?
d) What basic arithmetical and logical functions are used in SHA?

Problem2.

State the value of the padding field and the value of the length field in SHA-512 if the length of the message is

a. 2942 bits
b. 2943 bits
c. 2944 bits

Problem 3.

Suppose a message *m* is divided into *n* blocks of length 160 bits: $m = M_1 || M_2 || \ldots || M_n$. Let $h(x) = M_1 \oplus M_2 \oplus \ldots M_n$. Which of the properties (1), (2), (3) for a hash function does *h* satisfy and why?

(1) efficiency
(2) preimage resistant
(3) collision resistant

Problem 4.

Design a cryptosystem, which allows you to verify the message source and the message integrity when receiving a broadcast message (e.g., sent to all students from the student office). Plot the box diagrams for both the sender and the receiver and explain how the security requirements are addressed.

Problem 5.

Design a cryptosystem to send large messages with integrity check and encryption capabilities. You are only allowed to use a hash algorithm H. Public and symmetric crypto algorithms are prohibited. Assume the sender and the receiver have preshared a secret value, k. Explain how you use H and k to meet the security design requirements.

Problem 6.

1) How is a password stored in UNIX systems?
2) If adding a 12-bit salt in the UNIX password scheme, to what **maximal** factor can the system increase the difficulty of guessing a user's password?
3) But the salt is stored in plaintext in the same entry as the corresponding ciphertext password. Therefore, those two characters are known to the attacker and need not be guessed. Why is it asserted that the salt increases security?
4) Assume that passwords are limited to the use of the 95 printable ASCII characters and that all passwords are 10 characters in length. Assume a password cracker with an encryption rate of 6.4 million encryptions per second. How long will it take to exhaustively test all possible passwords on a UNIX system? What is the result if there are 10K password entries and 12bit salts are added to store the passwords?

Problem 7.

Design a secure cryptosystem and plot the box diagrams for both sender and receiver. Explain how and where your system meets the design goals: 1) confidentiality, 2) integrity, 3) authentication, and 4) addressing the security hole.