Additional Questions for Practice

You can get feedback and the answers if you make a serious attempt at answering the questions, and send your answers to me.

Symmetric Crypto

Consider the following mode of operation for a block cipher.

$$C_1 = IV \oplus E(K, P_1)$$
$$\cdots$$
$$C_i = C_{i-1} \oplus E(K, P_i)$$

Give the equations of the corresponding decryption, and identify two weaknesses of this mode of operation.

Integrity

One

Let $E(K, M)$ be the AES encryption of message M under key K. Suppose CBC is used and M could be longer than 128 bits. Let H be a hash function. Alice wants to send some secret information to Bob. To ensure data confidentiality and message authentication, Alice is to choose one of the two approaches below.

Approach 1: Send $E(K, H(M))$ to Bob

Approach 2: Send $E(K, M) \| E(K, H(M))$ to Bob

where the symbol $\|$ represents binary string concatenation. After doing some security analysis, Alice finds that one approach is flawed. Identify the flawed one and use at most 5 sentences to explain why it is flawed.

Two (SHA is SHA-1 with hash output length 160, and MD5 is hash length 128)

Find the expected number of messages that a bruteforce attacker has to try for breaking the collision resistance of the hash function H below. Represent your result in 2's power.

$$H(x) = \text{SHA}(\text{MD5}(x) \,||\, \text{MD5}(x) \,||\, \text{MD5}(x)).$$

Authentication/Key Management

Besides the following challenge-response method which can be used for one-way authentication, describe four other methods which only use symmetric key cryptographic techniques. You may use E (for symmetric key encryption), MAC (for message authentication code), and D (for symmetric key decryption).

$$A \rightarrow B : N$$
$$A \leftarrow B : H(K, N)$$

where N is a nonce and $H(K, N)$ denotes the hash of the concatenation of a symmetric key K pre-shared between A and B, and the nonce N. The protocol above allows A to authenticate B.

Network Security

One

For this question – what is the effort for active attacker to get correct SRES for specific mobile phone? Assume active attacker can interact with phone and network.

In GSM authentication, one of SRES and RAND is only 32 bits long while the other one is required to be 128 bits long. Identify the one which requires only 32 bits and the one which requires 128 bits. Also find out the probability that an active adversary is able to guess the value of SRES correctly.

In a system, each user has an entry in the system's password file: (y, s) where y is computed as follows and s is a salt.

i. $y = H(password, s)$ where H is SHA-1
ii. $y = H(s, password) \oplus password$
iii. $y = H(s) \oplus H(password)$
iv. $y = E(s, password)$ where E is AES and the first input of E is the key
v. $y = E(password, s)$
vi. $y = E(s, H(password))$
vii. $y = MAC(s, password)$ where MAC is HMAC and the first input of MAC is the key
viii. $y = MAC(password, s)$

List which of the methods above for computing y are secure against (precomputed) dictionary attack. Assume that s is 40 bits long and randomly chosen.