General Problems

1. Assuming you can do $2^{20}$ encryptions per second and the key size is 40 bits, how long would a brute force attack take? Give a scenario where this would be practical and another where it wouldn’t. What happens if you double the key size?

2. State Kerckhoff’s principle. Explain briefly why a cryptosystem designed by someone who follows this principle is likely to be stronger than one designed by someone who does not.

3. This very simplistic RSA encryption uses public key $(n=33,e=17)$ and encodes text one character at a time using the following numeric codes for each character:
   
   From 1 to 26 is a to z, 27 = . 28 = , 29 = ; 30 = ! 31 = ? 32 = -
   
   Show your working.
   
   (a) Encrypt ”edith”
   
   (b) What is the RSA private key?
   
   (c) Decrypt ”ml.z”

4. The following is from http://www.mail-archive.com/cryptopp-list@eskimo.com/msg01009.html
   
   Rijndael Encryption with SHA256 hash
   
   * From: Phillip Allan-Harding
   
   * Subject: Rijndael Encryption with SHA256 hash
   
   * Date: Wed, 30 Apr 2003 12:42:19 -0400 (EDT)
   
   I am relatively new to cryptography. Can someone comment on whether what I want to do sounds "correct" (whatever correct means!)
   
   - I want to encrypt data, that is to be transmitted around the inter/intraNet, using Rijndael
   
   - I want to use a key for the encryption that is an SHA128/256 hash based on:
     
     {multiple concatenated string data components} + {a nonce}
   
   Regards,
   
   Phil Allan-Harding.

   Give your comments:
5. Consider a server-assisted mutual authentication and key establishment protocol. Assume that Alice and the Server share a pairwise symmetric key $K_{AS}$, while Bob and the Server share a pairwise symmetric key $K_{BS}$. During the protocol, the trusted Server generates a fresh, random session key $K$ and distributes it to both Alice and Bob as follows:

Alice to Bob: $A, N_A$  
Bob to Server: $B, \text{enc}_{K_{BS}}(A, N_A, N_B)$  
Server to Alice: $\text{enc}_{K_{AS}}(B, N_A, K), \text{enc}_{K_{BS}}(A, K), N_B$  
Alice to Bob: $???$

6a. What message does Alice send to Bob in step 4 of the protocol?

6b. Suppose the second message of the protocol (from Bob to Server) is changed to $B, \text{enc}_{K_{BS}}(A, N_A)$. In other words, Bob’s nonce $N_B$ is not encrypted. Is the protocol still secure? Explain.

6. It is possible to use a hash function to construct a block cipher with a structure similar to DES. Because a hash function is one way and a block cipher must be reversible (to decrypt), how is it possible?

Now consider the opposite problem: using an encryption algorithm to construct a one-way hash function. Consider using RSA with a known key. Then process a message consisting of a sequence of blocks as follows: Encrypt the first block, XOR the result with the second block and encrypt again, etc. Show that this scheme is not secure by solving the following problem. Given a two-block message $B_1, B_2$, and its hash

$$\text{RSAH}(B_1, B_2) = \text{RSA}(\text{RSA}(B_1) \oplus B_2)$$

Given an arbitrary block $C_1$, choose $C_2$ so that $\text{RSAH}(C_1, C_2) = \text{RSAH}(B_1, B_2)$. Thus, the hash function does not satisfy weak collision resistance.

7. Is it necessary to recover the secret key in order to attack a MAC algorithm?

8. What changes in HMAC are required in order to replace one underlying hash function with another?

9. In regard to suppress-replay attack

   a) Give an example of an attack when a party's clock is ahead of that of the KDC.
   b) Give an example of an attack when a party's clock is ahead of that of another party
Bonus Question

10. Jamshid wants to give the directions to a secret weapon to his colleagues Saeed, Madjid and Kamran. The message $M$ is $n$ bits long. He suspects one of them may be a double agent, so he divides the message as follows:

- Saeed gets $K_1$, an $n$-bit random sequence.
- Kamran gets $K_2$, an $n$-bit random sequence.
- Madjid gets $C = K_1 \oplus K_2 \oplus M$

a. How can Saeed, Kamran and Madjid determine $M$? Prove that your method works.

b. Is the scheme secure? Argue convincingly that either

(1) It is secure - no two people can determine any bit of $M$ with probability greater than 0.5; or

(2) It is insecure - two people can conspire to determine a bit of $M$ with probability greater than 0.5.

Regulations and deadline

No hard copy is accepted unless by permission of respectful professor. You may send your solutions to either Sobhdel@nsc.sharif.edu or Sobhdel@ce.sharif.edu. You may name the file based on following formula:

<Your_Student_Number> + “_” + DNS_Assignment + <HomeworkNo>

For example: 87785665_DNS_Assignment1

Due date: 3 Weeks