Written Assignment

Some questions in this assignment come from the textbook: `Information Security Principles and Practice`. Nevertheless, you don't need to read the textbook in order to solve the questions.

This assignment has in total 100 points. That will count 10% of your final grade.

1. (5pt) With a Simple Substitution Cipher, find the plaintext and the key that correspond to the following ciphertext: dxjblsbo

2. (6pt) Using the letter encodings in Table 1, the following ciphertext message was encrypted with a one-time pad: `kite`.

letter	e	f	h	i	k	l	r	t
binary	000	001	010	011	100	101	110	111

Table 1: Alphabet encoding.

   (a) (3pt) If the plaintext is "here", what is the key?

   (b) (3pt) If the plaintext is "file", what is the key?

3. (6pt) Suppose that we have a computer that can test 2^{30} keys each second.

   (a) (2pt) What is the expected time (in years) to find a key by exhaustive search if the key has 80 bits?

   (b) (2pt) What is the expected time (in years) to find a key by exhaustive search if the the key has 100 bits?

   (c) (2pt) What is the max time (in years) to find a key by exhaustive search if the the key has 256 bits?

4. (8pt) This problem deals with the A5/1 cipher.

   (a) (2pt) On average, how often does the Y register step? And why? Please explain your answer.[1]

   (b) (2pt) On average, how often does exactly one register step? Please explain your answer.

   (c) (2pt) On average, how often do exactly two registers step? Please explain your answer.

[1] consider use a truth table to list all the inputs/outputs of the "majority voting" scheme we discussed in the lecture.

(d) (2pt) On average, how often do register X and Y step at the same time? Please explain your answer.

5. (18pt) Consider a Feistel cipher with four rounds. Then the plaintext is denoted as $P = (L_0, R_0)$ and the corresponding ciphertext is $C = (L_4, R_4)$. What is the ciphertext C, in terms of L_0, R_0, and the subkey[2], for each of the following round functions?

   (a) (2pt) $F(R_i, K_i) = 0$

   (b) (3pt) $F(R_i, K_i) = R_i$

   (c) (5pt) $F(R_i, K_i) = K_i$

   (d) (8pt) $F(R_i, K_i) = R_i \oplus K_i$

6. (6pt) Compared with ECB mode, please explain the advantage of CBC mode. In case certain blocks of ciphertext are tampered during transition when using CBC mode, do you see any problem? On the other hand, when certain blocks of ciphertext are tampered during transition when using ECB mode, do you see any problem?

7. (10pt) Let the encrypt function of standard DES be $C = E(P, K)$ where C is the ciphertext, P is the plaintext, and K is the key. Accordingly, let the decrypt function of DES be $P = D(C, K)$.

   Suppose that Alice uses a customized cipher $C' = D(E(P, K_1), K_2)$ where K_1 and K_2 are two keys, and Alice then sends C' to Bob. Suppose an attacker happens to know the plaintext P, but he does not know the two keys that was used in the cipher.

   (a) (2pt) What are the sizes of K_1 and K_2?

   (b) (6pt) Suppose an attacker knows the cipher text C'. Show that the attacker can figure out the two keys. Please elaborate your attack with diagrams.

   (c) (2pt) How could you modify the customized cipher and improve its security without adding another key? Why it becomes more secure? Please explain your answer.

8. (14pt) Suppose that Alice's RSA public key is $(N, e) = (91, 17)$.

   (a) (3pt) What is the value of Alice's private key?

   (b) (3pt) Please briefly explain why recovering the private key is hard.

   (c) (4pt) If Bob encrypts the message $M = 19$ using Alice's public key, what is the ciphertext C? Show that Alice can decrypt C to obtain M.

   (d) (4pt) Let S be the result when Alice digitally signs the message $M = 25$. What is S? If Bob receives M and S, explain the process Bob will use to verify the signature and show that in this particular case, the signature verification succeeds.

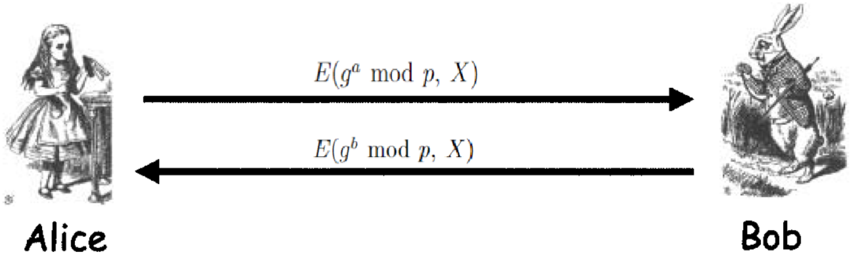
[2] Represent C with L_0, R_0, K_0, K_1, K_2, and K_3.

9. (9pt) Suppose that Bob uses the following variant of RSA. He first chooses N, then he finds two encryption exponents e_0 and e_1 and the corresponding decryption exponents d_0 and d_1. He asks Alice to encrypt her message M to him by first computing $C_0 = M^{e_0} \pmod{N}$, then encrypting C_0 to obtain the ciphertext, $C_1 = C_0^{e_1} \pmod{N}$. Alice then sends C_1 to Bob.

   (a) (3pt) Does this double encryption increase the security as compared to a single RSA encryption?

   (b) (6pt) Why or why not?

10. (8pt) Suppose that Alice and Bob share a 4-digit PIN number, X. An approach to establish a shared symmetric key with Diffie-Hellman is using the X to encrypt packages for key exchange. That is, Alice computes and sends $E(g^a \bmod p,\, X)$ and Bob computes and sends $E(g^b \bmod p,\, X)$.



   (a) (2pt) Is this new Diffie-Hellman method secure from the man-in-the-middle attack?

   (b) (6pt) Please explain why it is secure or not.

11. (10pt) Please elaborate the differences between crypto hash and encryption.

Submission Instructions

All submissions should be done through the Canvas system. You should submit a pdf document with your answers for each question.

It is important to name your files correctly. Please check out the late submission policies on the course website (https://course.cse.ust.hk/comp3632) in case you didn't attend the first lecture.