EECS 565 Intro Information & Computer Security

Homework 1: Cryptography

Your name:

Classic ciphers.

1. A substitution cipher replaces each letter with the one at the *i*-slots to its right. Please use the key "DAWN" to decrypt the ciphertext "vealruwgwwk". Show your decryption process briefly. Assume the letter "A" is mapped to position "0". A detailed mapping is provided as follows.

Position	0	1	2	3	4	5	6	7	8	9	10	11	12
Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Position	13	14	15	16	17	18	19	20	21	22	23	24	25
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

2. What is polyalphabetic substitution cipher? Compared with shift cipher, discuss two major differences between the two ciphers.

3. One-time pad is used to encrypt messages. If an attacker obtains the ciphertext and the corresponding plaintext message, can he find the encryption key? Does this mean OTP is vulnerable to the known-plaintext attacks?

4. What is frequency analysis? Please use frequency analysis to crack the below ciphertext. You can use tool to help compute the statistics, https://www.ittc.ku.edu/~fli/565/frequency_analysis.html.

   o kewixn zol yg yomn wnokvpn gt o sgvfypl ek yg xggm oy bgz wofl zofy ef ofq bgz wofl zofy gvy ygfl jxoep

   Hint: O=A, G=O, X=L, W=M, Y=T

Secret-key cryptography.

5. What is the block size and key length in DES encryption? Can two different keys encrypt the same plaintext into the same ciphertext? Why or why not?

6. What is the meet-in-the-middle attack? Please briefly explain why double-DES is vulnerable to this attack, but triple-DES is not.

7. What is the key exhaustive attack? If an attacker uses this attack to break a ciphertext encrypted by AES-192-CBC. Assume he uses a computer with 4GHz CPU to crack the keys and it takes about 100 cycles to test one key. How much time **on average** does he need to find the correct encryption key?

8. Errors in one block will propagate to other blocks when the CBC mode is used in block ciphers.
    a. Suppose an error occurs during transmission. One bit of the first ciphertext block is wrong. When the receiver tries to recover the message, how many plaintext blocks cannot be decrypted correctly?
    b. Suppose a one-bit error occurs in the first block of the plaintext message. After encrypting the message, how many ciphertext blocks will have error bits? When the receiver recovers the message, how many plaintext blocks cannot be decrypted correctly?

Public-key cryptography

9. Use RSA to encrypt the message "EECS". Assume p = 3 and q=11, and e=7. Please show the encryption steps (assume A=1). What is the security problem with textbook RSA encryption?

10. The Diffie-Hellman key negotiation protocol is vulnerable to the man-in-the-middle attack. Please explain the attack process and the mitigation methods.

11. SHA-256 is commonly used as the signing algorithm on SSL certificates. Which hash properties are desired in this use case? To successfully generate a collision (i.e., two certificates with the same signature), how many attempt **on average** should the attacker try (assume the desired collision probability is greater than 50%)?

12. What is HMAC? Find one use case of HMAC in real-world applications. Which hash property/properties is utilized by this application?