EECS 565 Intro Information & Computer Security

Homework 1 (each question is 10 points)

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

Answer: First, divide the ciphertext into 4-character blocks. Then, apply the key "DAWN" to each block and decrypt the ciphertext block by block.

The 1st block is veal, which is decrypted as:

v-d: 21-3 (mod 26) = 18 → S

e-a: 4-0 (mod 26) =4 → e

a-w: 0-22 (mod 26) =4 →e

l-n: 11-13 (mod 26) =24→y

The plaintext is: seeyouattwo

2. What is polyalphabetic substitution cipher? Compared with shift cipher, discuss two major differences between the two ciphers.
Answer: It's substitution cipher using multiple substitution alphabets.

Major differences: (1) it's a substitution cipher that permutate the input according to a substitution scheme (mapping). Shift ciphers use a substitution pattern based on letter shift. (2) multiple alphabets are used to map the same input letter to different output letters. This is to obfuscate the distribution of letters in the ciphertext based on their usage frequency.

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?

Answer: Yes, he can find the encryption key for the ciphertext that he obtains.

No, OTP is still secure as long as the key is not reused. OTP resists to known-plaintext attacks, because the keys for different messages are randomly generated.

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

   Answer: In cryptography, frequency analysis is the study of the frequency of letters or groups of letters in a ciphertext. Frequency analysis is based on the fact that, in any written language, certain letters and combinations of letters (e.g., bigrams) occur with varying frequencies. Moreover, there is a characteristic distribution of letters that is roughly the same for almost all samples of that language. Frequency analysis is used to break classical ciphers.

   The recovered plaintext: “A simple way to take measure of a country is to look at how many want in and how many want out”

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?

   Answer: DES has blocks of 64 bits and uses keys of 56 bits long (8 bits are parity). Given a plaintext, we can map (or transform) it to a specific ciphertext output. Two different keys will always generate two different ciphertexts.

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.

   Answer: In the meet-in-the-middle attack, the attacker attempts to simultaneously encrypt the plaintext and decrypt the ciphertext, and then looks for a match between two intermediate outputs. One from the attempted encryption process and the other from the attempted decryption process. Since the attacker attempts to break the cipher from both directions, it is named meet-in-the-middle.

   Double-DES is vulnerable to this attack. Given a pair of plaintext and ciphertext, the attacker only needs to encrypt the plaintext with all possible values of the keys and decrypt the ciphertext with all possible keys and look for the match between two sets of results. Compared with the brute force attack against DES, this attack requires only one additional encryption/decryption operation at each step. It only doubles the computation load of the attacker, which means increasing the security strength by a factor of 2.

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?

   Answer: In a key exhaustive attack, all possible keys are tested to decrypt the ciphertext. The keyspace for AES-192 is 2^192. On average, you can break a cipher by searching half the key space. So, the attacker needs to search 2^191 keys. The computing speed is 4x10^9 cycles per second. It can compute 4 x10^9/100 = 4x10^7 keys per second. So, the time to crack the key is 2^191/4 x 10^7 = 2^189 x10^-7 seconds = 7.84 x 10^49 seconds.

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?

   Answer: In CBC, the error in C1 will cause complete corruption in the decrypted plaintext block (i.e., P1). C1 will be used in the decryption of C2, so the decrypted plaintext block P2 will be incorrect. Since C2 does not have any error bits, the decryption of C3 (and the rest of the blocks) will remain intact.

   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?

   Answer: If one bit error occurs in the plaintext block P1 (denoted as P1'), all the ciphertext blocks (i.e., C1', C2', etc.) will be different from original correct ciphertext blocks (C1, C2, etc.). However, when the receiver decrypts the received ciphertext blocks C1', C2', etc., he can recover all the plaintext blocks correctly except the first one P1, which has one bit error.

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?
   Answer: First, compute n=p*q=33. The public key is <e, n> = <7, 33>. Next convert "EECS" into numbers as

   E=5, C=3, S=19.
   E: 5^7 mod 33 = 14.
   C: 3^7 mod 33 = 9.
   S: 19^7 mod 33 = 13.
   So, EECS is encrypted as 14, 14, 9, 13.

   The output of RSA is deterministic. So, the same plaintext E generates the same ciphertext. If the plaintext space is known and small, the attacker can try all possible plaintexts. To mitigate the attack, we need to use padding to pad short plaintext message.

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.
    Answer: In the D-H protocol, a mitm attacker can impersonate Alice to Bob and simultaneously impersonate Bob to Alice. Therefore, he can exchange his public element with Alice and Bob, respectively. As a result, he can negotiate a secret session with Alice and Bob, respectively. Later, he uses the secret key with Alice to decrypt the message encrypted by Alice and uses the secret key with Bob to encrypt the plaintext message and sends it to Bob. Neither Alice nor Bob would notice these actions.

    This attack can work because the D-H protocol does not support authentication. It can be mitigated if additional authentication is provided to prove the authenticity of the exchanged public elements, such as using authenticated D-H exchange or using published DH numbers.

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%)?
    Answer: We use two hash properties here: Collision resistance and weak collision resistance.

    Following the birthday attack calculation, the brute force collision search requires O(2^(m/2)) computation. Here m=256, so the average attempts is 2^128.

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

    Answer: HMAC is a massage authentication code (MAC) based on keyed hash. It takes the message and a secret key as the input to a one-way hash function and produces the output as the MAC. HMAC is used in many applications:

    - It is used in SSL/TLS to encapsulate the IP header for integrity.
    - Used in IPsec for message authentication.
    - Used in digital signatures to compress the message into a smaller-sized form to be signed.
    - Used in password hashing to hash the password with a key for secure password storage.