Search

Your name (First Last): .....

Question 1 (38 pts, 2 pt each space) Fill in each of the underlined empty spaces with one word, a short phrase, or some number(s).

- The main weakness in substitution ciphers is Vulnerable to freq analysis
- The key space (i.e. number of possible keys) in a shift cipher (i.e. Caser Cipher) to encrypt English language plain text is 25.
- In stream ciphers where the keystream generator produces keystream $[K_1, K_2, ..., K_n]$ to encrypt plaintext $[P_1, P_2, ... P_n]$, the ciphertext will be $C_i =$ $P_i \oplus K_i$.
- Among the 3 encryption modes (ECB, CBC & CTR) for block ciphers, CBC offer(s) randomized encryption, CTR can use parallelism to speed up encryption. (List all that apply in both spaces.)
- The Data Encryption Standard (DES) has a block size length of 64 bits bits and a key size of 56 bit bits.
- Conceptually, the HMAC function using a hash function h, a key K and a message M can be written as $\text{HMAC}_K(M) =$. (Give the high-level view of the formula.)

Search

Midterm Exam (Time: 60 minutes)

Your name (First Last): .....

Question 1 (38 pts, 2 pt each space) Fill in each of the underlined empty spaces with one word, a short phrase, or some number(s).

- The main weakness in substitution ciphers is _____.
- The key space (i.e. number of possible keys) in a shift cipher (i.e. Caser Cipher) to encrypt English language plain text is _____.
- In stream ciphers where the keystream generator produces keystream $[K_1, K_2, ..., K_n]$ to encrypt plaintext $[P_1, P_2, ... P_n]$, the ciphertext will be $C_i =$ _____.
- Among the 3 encryption modes (ECB, CBC & CTR) for block ciphers, _____ offer(s) randomized encryption, _____ can use parallelism to speed up encryption. (List all that apply in both spaces.)
- The Data Encryption Standard (DES) has a block size length of _____ bits and a key size of _____ bits.
- Conceptually, the HMAC function using a hash function h, a key K and a message M can be written as $\text{HMAC}_K(M) =$ _____. (Give the high-level view of the formula.)

5:19 PM

- The Data Encryption Standard (DES) has a block size length of _____ bits and a key size of _____ bits.
- Conceptually, the HMAC function using a hash function h, a key K and a message M can be written as $\text{HMAC}_K(M) =$ $h(K \| h(K \| M))$. (Give the high-level view of the formula.)
- In the RSA **encryption** algorithm, the public encryption key is (n, e), and the private decryption key is d, where n is the product of two large prime numbers. To encrypt a message M, one computes the ciphertext $C =$ $m^e \bmod n$. To decrypt C, one computes $C^d \bmod n$. Knowing $n = pq$, the decryption key d can be computed from p, q, e by solving $ed \equiv 1 \bmod \phi(n)$.
- In the Diffie-Hellman protocol, Alice and Bob want to agree on a shared secret. They have two public numbers; a generator g and a large prime number p. Alice chooses (a) at random and sends $g^a \pmod p$ to Bob, and Bob chooses (b) at random and send $g^b \pmod p$ to Alice, the shared secret is $g^{ab} \pmod p$.

- Concepts in access control include subjects, objects, and principals. In UNIX system, subjects are manifested as _____, objects as _____, and principals as _____.
- In current UNIX, the _____ of a file can change the permission bits of the file, and the _____ can change the owner.

Question 2 True/False Questions (20 pts, 2 pts each) Circle yes or no.

yes / no Encryption keys need to always be kept secret to maintain the security of a cryptosystem.

yes / no The substitution cipher is insecure even in a ciphertext only attack.

yes / no The main vulnerability is the subsituation cipher is that they key space is too small.

yes / no A Pseudo Random Number Generator is actually a deterministic function such that the same input (seed) will always result in the same output stream.

yes / no Hash functions provide integrity of communicated information.

yes / no The security of public key encryption requires that knowing the public key, it is computationally infeasible to compute the private key.

yes / no Both message authentication code and digital signatures can provide authentication and non-repudiation.

yes / no Public salting passwords increases the difficulty to launch a dictionary attack against a single user account.

yes / no Biometrics are secure way of authentication as they provide a deterministic measure of identity

yes / no The security of public key encryption requires that knowing the public key, it is computationally infeasible to compute the private key.

yes / no Both message authentication code and digital signatures can provide authentication and non-repudiation.

yes / no Public salting passwords increases the difficulty to launch a dictionary attack against a single user account.

yes / no Biometrics are secure way of authentication as they provide a deterministic measure of identity.

yes / no Using "input validation" to reduce applications vulnerabilities, it is better to *blacklist* what is not allowed that *whitelisting* what is allowed.

Question 3: Fill in empty cells (9 pts) For each empty cell in the table below, answer whether the defense mechanism listed in the column help defend against the kind of attack in the row. Just write **yes** or **no** in each cell.

	Non-executable Stack
Basic buffer-overflow with shell code on stack	yes
Return to libc	no
Overflow function pointers in current stack frame to point to the system library function	no

Question 3 (2 pts) Order each of the following in ascending order (smaller first).

(2 pts) Order the following classical ciphers with respect to the size key space (i.e. number of possible keys).

1. Substitution cipher.
2. Vigenere cipher (with key length = 10)

2 → 1

Question 4 (6 pts) Circle the most correct answer of each of the following statements [only choose one].

- Because of birthday attacks the length of hash function outputs should _____ the key length of block ciphers to achieve equivalent security:
  1. be the same as.
  2. half of.
  3. double.
  4. triple.
- Message Authentication Codes (MACs) mainly provide us with _____.
  1. Data Integrity
  2. Data Encrytion
  3. Data Origin Authentication
  4. Data Avaialbility

Question 4: Choice Questions (10 pts)

For the following types of malwares, identify the numbers corresponding to their definitions from the list below them:

- rootkit: (5)
- botnet: (4)
- ransomware: (3)
- worm: (1)
- spyware: (2)

The list below gives definitions of some malware types.

1. Malware that self-propagates
2. Malware that collects information about users without their knowledge
3. Malware that holds a computer system, or the data it contains, hostage against its user by de-

1. Malware that self-propagates
2. Malware that collects information about users without their knowledge
3. Malware that holds a computer system, or the data it contains, hostage against its user by demanding a payment
4. A collection of compromised machines under a central command and control center
5. Malware that actively hide its presence from administrators by subverting standard operating system functionality or other applications
6. Malware that use fake warnings to scare users into paying for products.

Question 5: Short Answer Questions (17 pts)

(5 pts) Steam ciphers create a key-stream from a small fixed key. Are stream ciphers secure if the same key-stream used twice? Why (write the encryption formulas)

if used twice be easy to break

$C1 = P1 \text{ xor } K1$

$\overline{C1} = \overline{P1} \text{ xor } K1$

$K1 = C1 \text{ xor } P1$

$K1 = \overline{C1} \text{ xor } \overline{P1}$

$\overline{C1} \text{ xor } \overline{P1} = C1 \text{ xor } P1$

$C1 \text{ xor } \overline{C1} = P1 \text{ xor } \overline{P1}$ → better than 50%

(4 pt) Cryptographically secure pseudo-random number generator requires unpredictable sequences. One requirement is that it satisfies the "next-bit" test. What is this test?

(4 pt) Cryptographically secure pseudo-random number generator requires unpredictable sequences. One requirement is that it satisfies the "next-bit" test. What is this test?

(4 pts) Suppose that a bank assigns randomly generated passwords to online banking users in order to avoid users choosing weak passwords. What are the main shortcomings of this approach?

(4 pts) Suppose that a bank assigns randomly generated passwords to online banking users in order to avoid users choosing weak passwords. What are the main shortcomings of this approach?

(4 pt) Cryptographically secure pseudo-random number generator requires unpredictable sequences. One requirement is that it satisfies the "next-bit" test. What is this test?

(4 pts) Suppose that a bank assigns randomly generated passwords to online banking users in order to avoid users choosing weak passwords. What are the main shortcomings of this approach?

(4 pts) Suppose that a bank assigns randomly generated passwords to online banking users in order to avoid users choosing weak passwords. What are the main shortcomings of this approach?

(4 pts) Explain an attack one can perform by changing the IFS environment variable.

(4 pts) Explain an attack one can perform by changing the IFS environment variable.

Good luck :-)