CS 370 / ECE 499 Computer Security

Sample Final

Please read the following rules before starting.

- This is just a list of sample question so yo know what to expect. Don't too much into coverage of topics.
- This together with midterm and problem sets should give a pretty good idea of what to expect
- The final exam may have most questions as multiple choice questions with space for justification or explanation of your choice.

PRINT NAME : ____

PRINT OSU ID : ____

SIGNATURE : ____

Fast Problems

1. **(2 pts)** For each statement below about threats and security property violations, circle true (T) or false (F).

   - (F) *Snooping* is a threat to data integrity
   - (F) *Spoofing* is a threat to system availability

2. **(2 pts)** Which hash algorithm would be most appropriate for generating hash of a software package to be distributed on public servers? In this scenario software may be hosted on public mirror sites while the hash is posted on the secure corporate website. (circle one answer from below)

   A. SHA-2

   B. HMAC-SHA2

   C. CRC

   D. RSA

3. **(2 pts)** The number of steps in a brute force attack on a system that is using double DES with two keys to encrypt the plaintext is:

   A. 2^{56}

   B. 2^{57}

   C. 2^{112}

   D. 2^{128}

4. **(2 pts)** In the table below match the desired security requirement or property with cryptographic primitives or tool that can provide that property. Enter the letter index of the matching primitive next to the property in first column. Each letter index can only be used once.

Security Property / Requirement	Cryptographic Primitive/Tool
Origin Integrity [D]	A. Block Cipher
Confidentiality [A]	B. Digital Signatures
Non-repudiation [B]	C. Cryptographic Hashes
Data Integrity [C]	D. HMAC

5. **(5 pts)** What is true of a *nonce* (circle all that apply)

   - It is included in a key exchange algorithm to defend against replay attacks
   - It needs to be kept confidential
   - It is often a random or a psuedo-random number
   - It is pre-shared

- It must contain enough bits to be distinguishable from all other nonces recently used.

6. **(4 pts.)** Circle T (true) or F (false) for each of the statements below regarding cryptographic hash functions and their use.

   - (T) If a hash function is to be used with an encryption algorithm whose key length is K, then the hash function ought to have $2K$ output bits.
   - (F) A hash function is said to be cryptographically secure if the number of its output bits is so large that collisions are impossible.
   - (F) All hash functions ever promoted by NIST standards are mathematically strong, in the sense that one can never do better than brute force in attempting to discover what input I maps to known hash value $h(I)$.
   - (T) Birthday attacks are ineffective against keyed cryptographic hash functions such as HMACs

7. **(2 pts)** Which of the following is the best example of multi-factor authentication? (circle one answer from below)

   A. Customer enters password on a bank's website and reviews a previously selected picture displayed by the bank?s website.

   B. Customer's browser verifies the validity of the bank's website?s certificate, and customer enters password.

   C. Customer enters a 6 digit pin on the secure card that his bank gave him, and the secure card displays a 12 digit code that the customer enters on the bank website.

   D. Customer enters a password on the bank's website.

8. **(2 pts)** Suppose you are working as the security administrator at *xyz.com*. You set permissions on a file object in a network operating system which uses DAC (Discretionary Access Control). The Extended ACL (AccessControl List) of the file is as follows:
   Owner: Read, Write, Execute
   User C: Read, Write, -
   User B: -, -, - (None)
   Sales: Read, -, -
   Marketing: -, Write, -
   Mask: Read, Write, -
   Other: Read, Write, -

   User "A" is the owner of the file. User "B" is a member of the Sales group.
   What effective permissions does User "B" have on the file?

   A. User B has no permissions on the file.

   B. User B has read permissions on the file.

   C. User B has read and write permissions on the file.

   D. User B has read, write and execute permissions on the file.

9. **(2 pts)** Which of the following statements is NOT true about Role-Based Access Control (RBAC)

   A. A user can be assigned one or more roles

   B. A session can have one or more users

   C. A session can have one or more roles

   D. A role can be assigned to one or more users

10. **(2 pts)** Consider a Role-Based Access Control (RBAC) system where a role **R1** and role **R2** are mutually exclusive roles. **R1** has permissions to perform operations **Review** and **Approve** on resource **Report**, and **R2** has permissions to perform operation **Edit** on resource **Report**. No other role in the system has permissions to perform any operation on resource **Report**. Which of the following statements CANNOT be true in this setting?

    A. Users Alice and Bob can both be assigned to **R1**.

    B. User Alice can be assigned to **R1** and user Bob can be assigned to **R2**.

    C. User Candice can **Edit** resource **Report** and **Review** her edits to **Report**

    D. Users Eve and Mallory can both be assigned to **R2**.

Not-So-Fast Problems

11. **(6 pts) Historical Ciphers**
Now imagine encoding a message using the Vignère cipher several times, each with a different keyword. Use this technique to encode the message 'SECRET' four times, using the keywords (in sequence) 'PWORDA', 'PWORDB', 'PWORDC', 'PWORDD'.
Similar to your mid-term problem where you add the keys to find the final key (shift). Add PWORDA + PWORDB + PWORDC + PWORDD modulo 26 to get the final KEY and use that KEY to encrypt using Vignère cipher.

12. **(5 pts) DES**

A triple-DES machine does three DES operations in the following sequence:

(a) an encode stage using some key k1,

(b) a decode stage using some key k2,

(c) a final encode state using key k3.

A user configures the machine so that $K1 = k2 = k3$.

(2 pts) The effective strength of the machine under this configuration is (choose one)

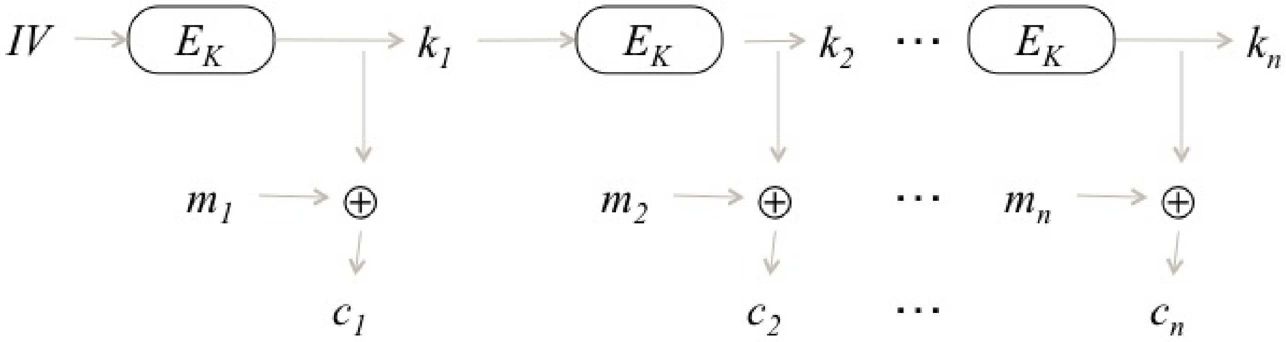
A. The same as single stage DES, 56 bits. This is a backwards compatible 3DES

B. Effectively 57 bits, because this configuration is subject to a meet-in-the-middle attack

C. No security because the encryption and decryption operations cancel out.

(3 pts) Justify or explain your selected answer.

the last two stages (or the first two) - decode and encode - cancel out each other as they are using the same key, i.e., k3 = k2 (or k1 =k2)

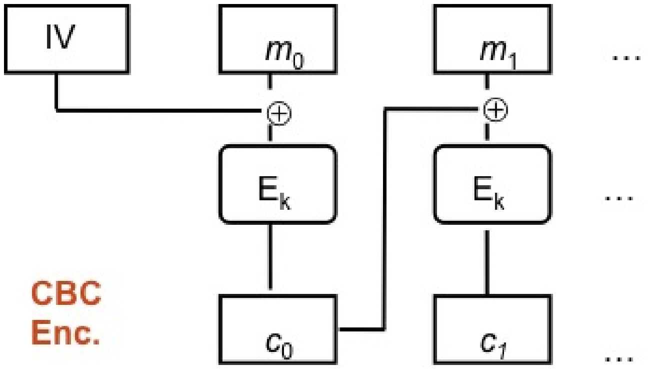


13. **(12 pts) Encryption Modes 1**
Figure above shows a mode for encryption. Here IV represents the initialization vector, E_K represents encryption using a block cipher with key K, and $\oplus$ represents XOR operation.

(a) (4 pts) Identify the mode. Draw the corresponding decryption sequence. OFB. decryption diagram - swap m_i and c_i in the encryption diagram to get decryption diagram

(b) (4 pts) State four salient properties of this mode. (Hint: Compare it with other modes covered in class)
1. It randomizes the cipher-text output as long as the IV is random just like CBC.
2. Keystream is independent of both the plaintext and ciphertext and is only dependent on the IV - so unlike CBC it can be pre-computed to speed up encryption or decryption. But unlike CTR mode it is not parallelizable
3. It can convert a block cipher into a stream cipher.
4. It uses only the encryption function and doesn't need to use decryption function.

(c) (4 pts) Can this mode be used with public-key encryption? Specifically, can the block cipher E_K be replaced by a public-key primitive such as RSA? Why or why not?
No. Because this mode only uses enciphering function for both encryption and decryption, replacing the block cipher with public-key one like RSA means anyone with the public-key can decipher the message rendering the encryption useless in terms of protecting confidentiality.

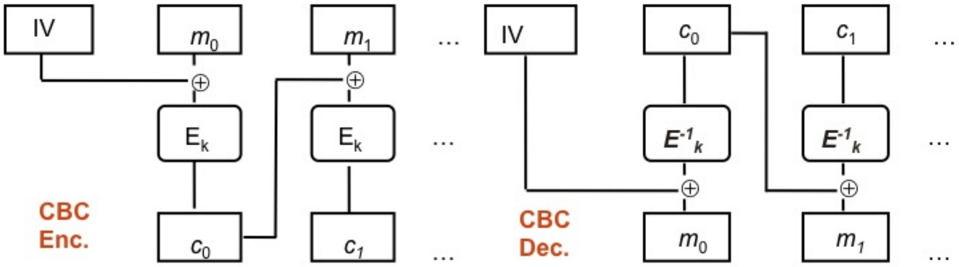


14. **(5 pts) Encryption Modes 2**
Figure above shows CBC mode for encryption. Here IV represents the initialization vector, and E_k represents encryption using a block cipher with key k respectively. CBC encryption can be described by the following equations

$$c_0 = E_k(m_0 \oplus IV)$$

$$c_i = E_k(m_i \oplus c_{i-1}) \text{ where } i > 0$$

Draw the figure for CBC decryption and write down the associated equations . Use E_k^{-1} to denote decryption with key k



$$m_0 = E_k^{-1}(c_0) \oplus IV$$

$$m_i = E_k^{-1}(c_i) \oplus c_{i-1} \text{ where } i > 0$$

15. **(8 pts + 5 Bonus) Crypto Primitives and Security Properties**
Alice and Bob share symmetric keys $K1_{AB}$, $K2_{AB}$ and each have an asymmetric key pair (SK_A,PK_A) and (SK_B,PK_B) respectively. Here SK_A denotes secret-key (also called private key) of Alice and PK_A denotes public-key of Alice. Recall the notation that $x||y$ means the concatenation of x with with y, $\{x\}_k$ denotes the the encipherment of of x using key k, $h(x)$ denotes a hash of x, and $MAC_K\{x\}$ demotes MAC of x with key K.

For each of the messages from Alice to Bob shown below identify what properties are provided. Choose one or more among {message integrity, origin authenticity, confidentiality, non-repudiation } and write them below each message in the space provided.

(a) (2 pts) $A \rightarrow B : m, \{h(m)\}_{SK_A}$;
Signed by Alice. message integrity, origin authenticity, non-repudiation

(b) (2 pts) $A \rightarrow B : \{m\}_{K1_{AB}}, \{m\}_{PK_B}$;
Encrypted twice by Alice. Once with symmetric key and once with public-key of Bob. Confidentiality

(c) (2 pts) $A \rightarrow B : \{m\}_{K1_{AB}}, MAC_{K2_{AB}}\{m\}$;
Encrypted and MACed by Alice using shared symmetric keys. message integrity, origin integrity and confidentiality

(d) (2 pts) $A \rightarrow B : \{m\}_{K1_{AB}}, \{h(m)\}_{SK_A}$
Encrypted using symmetric key and signed by Alice. message integrity, origin integrity, confidentiality, and non-repudiation

(e) (Bonus: 5 pts) In part C above where symmetric keys are used to provide security properties, identify of a weakness and suggest a fix.
MAC provide integrity protection and don't necessarily protect against information leakage. Therefore if both confidentiality and message integrity are desired, then the MAC should be applied either to the hash of the message or to the ciphertext.

16. **(6 pts) Hash Functions.**
Alice wants to send a message to Bob. She appended a digital signature with her message as shown - $m \| Sig(m)$

(a) (3 pts) Assume Eve intercepts the message. Assume she doesn't have access to Alice's private key SK_A. Assume Alice used a cryptographic hash function for signing her message. That is, $Sig(m) = \{h(m)\}_{SK_A}$. What security property of the hash function is crucial in preventing Eve from changing the message from m to m' while making it appear that Alice has signed the new message. Explain.

2nd pre-image resistance or weak-collision resistance; that is, given m, hard to find m' such that $h(m) = h(m')$; 3 pts

Strong Collision Resistance is not right answer as m is given; partial credit will be given for mentioning collision resistance

(b) (3 pts) If Eve wants to achieve the above attack using brute force, how would she go about this and roughly how many steps would this attack take? Assume that the hash function in use is SHA-256.

Eve would have to try different m' till she found one with $h(m') = h(m)$; 1.5 pts

By Pigeon hole principle this takes 2^{256} steps as SHA-256 has 256 bit output; 1.5 pts

Birthday attack is not right answer

17. **(24 pts) Misc.**

(a) (3 pts) Compare and contrast the following two security design principles: i) least-privilege and ii) separation-of-privilege

Least-privilege: Only granting the minimum privileges needed for a user to do his/her job. Separation-of-privilege: Ensuring that privileges needed to complete sensitive tasks are split between multiple users. Similarity: Both are meant to reduce the impact of a compromise of an account/user. Separation-of-privilege is also meant to reduce the chance of fraud by forcing multiple users to be involved, and increasing the chance of detection when fraud happens.

(b) (3 pts) What is the difference between Vulnerabilities and Threats?

Writing their definitions will highlight the difference.

(c) (3 pts) Name a security property that asymmetric-key cryptography can readily provide but symmetric-key cryptography cannot. Explain why.

Non-repudiation. Because in pub-key systems only the signer has access to the key that can produce a signature so a valid signature can be used as proof to provide non-repudiation. In symmetric-key systems both parties share a key so a valid MAC cannot be conclusive proof to show one of them did something - like sent a message

(d) (3 pts) What is the principle of complete mediation?

Principle of complete mediation says that every resource access needs to mediated by a security policy enforcement point. - 3 pts

(e) (3 pts) What is the difference between ACLs and Capabilities?

ACLs are a slice-by-column instantiation of an access control matrix, where as Capabilities are a slice-by-row instantiation of an access control matrix

(f) (3 pts) What is per-subject review? Is it easy to undertake per-subject review with ACLs or Capabilities? Explain.

Per-subject-review is reviewing all the accesses a given subject has in a system. It is easy to undertake per-subject review with Capabilities as capabilities capture the rows or an access control matrix, that is, all the access that a given subject is allowed.

(g) (3 pts) What is a TPM? What services does it provide?
Trusted Platform Module is a security co-processor that provides i) secure storage, ii)authenticated boot and iii) attestation

(h) (3 pts) What is sealing? Can data sealed by one TPM be unsealed by another?
Sealing is a way to store secrets leveraging a TPM generated key. No, data sealed by one TPM cannot be unsealed by another.

18. **(10 pts) Password Authentication**

   (a) **(5 pts)** You are designing a password system with randomly selected passwords. The alphabet for the passwords is the set of alphanumeric characters in English - lower case letters and the integers 0-9. You want to use passwords of exactly 12 characters. You are told that the attacker can make 450 billion guesses each minute. If the passwords are exactly 12 characters long, how long until the attacker has a 50% chance of correctly guessing a user's passwords in an offline attack.

   Using Anderson's formula $P = TG/N$. $P = 0.5$; $T = 24*60*365*Y$ minutes; $G = 450*10^9$; $N = 36^{12}$
   $T = PN/G \Rightarrow Y = (0.5*36^{12})/(450*10^9*24*60*365) \approx 10$ years

   (b) (5 pts) Describe 2 advantages and 2 disadvantages of using Biometrics for user authentication?

   advantages: biometrics are unique, good entropy (as opposed to weak passwords), always with user, ; 2 pts - 1 point per advantage disadvantages: expensive hardware, false positives/negatives, biometrics change over time, etc.; 2 pts - 1 point per disadvantage

19. **Access Control and RBAC**

   - A. (4 pts) What is "SetUID" in Unix? What is one advantage/pro and one disadvantage/con of using this feature?

     2 pts - SetUID is on of the 3 special protection bits in UNIX file system. When set on a file it indicates that when the file is executed by any authorized user that executing process be run with the privileges of the owning user.

     2 pts - Advantage: Programs needing privileged access can be run by users without having to give them all privileged access.
     Disadvantage: Possible vector for privilege escalation - if a program owned by root that has SetUID is compromised say through buffer overflow then the adversary gets root privileges.

   - Problem Set 3 provides a good guide for questions on RBAC and access control.

	File 1	**File 2**	**File 3**	**File 4**	**User A**	**User B**	**User C**
User A	Own R W		Own R W		control		
User B	R	Own R W	W	R*		control	own
User C	R W	R		Own R W			control

20. (**9 pts**) Keeping in mind the rules governing access control matrix change discussed in class, and the access matrix shown above, answer whether or not the following changes to access matrix are allowed. **Explain why or why not**.

- **(3 pts)** (allowed / not allowed) User A wants to **Grant** R^* on File 3 to User C User A owns File 3 so he is allowed to grant R/W access to File 3 to any user

- **(3 pts)** (allowed / not allowed) User A wants to **Revoke** rights of User C on File 2 Neither does User A own File 2 nor does he own User C, so he is not authorized to revoke User C's rights to File 2

- **(3 pts)** (allowed / not allowed) User C wants to (**Read**) the access rights of User B on File 4 User C owns File 4 so he/she is authorized to see who has what accesses to File 4.

21. **Key Exchange** Problem Set 3 provides sample questions on Key Exchange.

Vigènere Tableau

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y