CYBR 171: TEST 1

April 18, 2024

Instructions

- Time allowed: **60 minutes**
- **CLOSED BOOK**
- **Permitted materials**
  - Only silent non-programmable calculators or silent programmable calculators with their memories cleared are permitted in this test.
  - Printed English to foreign language dictionaries are permitted.
  - No other material is permitted.
- **Questions**
  - Attempt **ALL** questions in this booklet.
  - **ALL** questions are multichoice.
  - There will be more than **ONE** right answer, make sure you choose the **BEST** answer.
- You do **NOT** lose marks for incorrect answers.
- This test contributes 25% of your final grade.
- **Hand in the test booklet.**

Questions	**Marks**
1. Section A - KEY CONCEPTS	[10]
2. Section B - CLASSICAL CRYPTOGRAPHY	[10]
3. Section C - MODERN CRYPTOGRAPHY	[10]
4. Section D - AUTHENTICATION	[10]
5. Section E - MALWARE	[10]

This page intentionally left blank.

SECTION A - KEY CONCEPTS

Question 1. The Parkerian Hexad expands the CIA Triad. Name the THREE additional security properties it includes. [1 mark]

A. Authenticity, Accountability, Utility.
B. Possession, Authenticity, Utility.
C. Non-repudiation, Authenticity, Accountability.
D. Non-repudiation, Control, Availability.

Question 2. Which of these is NOT a typical characteristic of a white hat hacker? [1 mark]

A. Works within legal and ethical boundaries
B. Seeks permission before testing systems
C. May disclose vulnerabilities without authorization
D. Often reports findings to help improve security

Question 3. What's the MAIN difference between a passive and an active attack? [1 mark]

A. Active attacks are harder to detect.
B. Active attacks directly modify a system or its data.
C. Only active attacks can violate security properties.
D. There is no difference.

Question 4. Explain why a company offering online banking might implement a security policy that limits the number of failed login attempts before locking an account [1 mark]

A. This helps protect against brute-force password attacks.
B. It improves system availability by reducing traffic spikes.
C. It ensures the integrity of account data.
D. This is not a common security practice.

Question 5. Which of the following is a KEY advantage often held by insider threats compared to outsider threats? [1 mark]

A. Insiders have better technical knowledge of the system's vulnerabilities.
B. Insiders may already have authorized access to sensitive resources.
C. Insiders are less likely to be detected by standard security measures.
D. Insiders have more to gain from outsiders.

Question 6. A news website suffers a denial-of-service attack, making it inaccessible to readers. What aspect of the CIA triad is MOST likely violated in this scenario? [1 mark]

A. Availability.

B. Confidentiality.

C. Integrity.

D. Utility.

Question 7. An e-commerce website prioritizes a seamless user experience. They decide to minimize security prompts and store customer credit card information for faster checkouts. This decision PRIMARILY impacts the trade-off between? [1 mark]

A. Confidentiality and integrity.

B. Integrity and availability.

C. Confidentiality and availability.

D. Posession and confidentiality.

Question 8. You discover a vulnerability that allows unauthorized access to a hospital's database. You gained access without permission, informed the hospital of the issue, and no damage was done. According to the New Zealand law, which of the following statements is MOST likely to be correct regarding the legality of your actions?

A. Legal, as no financial or reputational harm was caused.

B. Legal, as your actions ultimately improved the hospital's security.

C. Not legal, as you performed unauthorized access, regardless of intent.

D. Not legal, as your actions were malicious, seeking personal gain.

Question 9. Which of the following BEST defines a cybersecurity threat as defined in the course material. [1 mark]

A. A weakness that could be exploited by an attacker.

B. Any action with the potential to harm a system.

C. A circumstance or event that could compromise security (CIA or Parkerian Hexad properties).

D. An attack that has already successfully compromised a system.

Question 10. How does non-repudiation help to prevent fraud in financial transactions? [1 mark]

A. It ensures that messages cannot be modified.

B. It ensures the confidentiality of messages.

C. It prevents a party from denying sending or receiving a message.

D. It prevents unauthorised access to messages.

SECTION B - CLASSICAL CRYPTOGRAPHY

Question 11. Which of the following is the process of transforming readable plaintext into unreadable ciphertext? [1 mark]

A. Steganography
B. Cryptanalysis
C. Transposition
D. Encryption

Question 12. Why is frequency analysis a useful technique for breaking simple substitution ciphers? [1 mark]

A. It works best when the key length is very long.
B. Letters in a language have predictable frequency distributions.
C. It relies on the use of electromechanical devices.
D. It's the only way to break one-time pads.

Question 13. What is the <u>KEY</u> difference between a substitution cipher and a transposition cipher? [1 mark]

A. Transposition ciphers are used with computers, while substitution ciphers are not.
B. Transposition ciphers are unbreakable, while substitution ciphers are not.
C. Substitution ciphers replace letters; transposition ciphers rearrange them.
D. Substitution ciphers use long keys; transposition ciphers use short keys.

Question 14. You want to encrypt a plaintext message: "ATTACK" using a Caesar cipher using a shift of 3. What is the ciphertext? [1 mark]

A. DWWDFN
B. WPPWYG
C. CVVCEM
D. XQQXZH

Question 15. A one-time pad cipher is considered theoretically unbreakable because: [1 mark]

A. It uses keys longer than the plaintext.
B. It was used by the Enigma machine.
C. The key is truly random and used only once.
D. It employs both substitution and transposition techniques.

Question 16. According to Claude Shannon, which of the following is MOST important to kept secret? [1 mark]

A. Algorithm.

B. Encryption system.

C. Key.

D. Number of possible keys.

Question 17. The Vigenère Cipher is stronger than the Caesar Cipher MAINLY because: [1 mark]

A. It uses longer keys.

B. It changes the substitution pattern for each letter.

C. It involves electromechanical components.

D. The key is as long as the message itself.

Question 18. You want to encrypt a plaintext message: "ATTACK" using a Vigenère cipher with the keyword "DAY". What is the ciphertext? [1 mark]

A. DWWDFN

B. DTRDCI

C. DTRAFK

D. YTWYCN

	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

Figure 1: Vigenère table for question 18

Question 19. Why are one-time pads difficult to implement perfectly in practice? [1 mark]

A. Perfect randomness is impossible to achieve.

B. Frequency analysis remains effective against them.

C. Keys must be very short to be secure.

D. Generating and managing truly random, long keys is challenging.

Question 20. Which of the following factors was the <u>MOST</u> crucial in the initial stages of breaking the Enigma code? [1 mark]

A. The development of advanced electromechanical deciphering machines known as Bombes.

B. The capture of Enigma machines and codebooks from German U-boats.

C. The exploitation of a flaw in German operational procedures regarding message keys.

D. The recruitment of Polish mathematicians who had reverse-engineered earlier Enigma versions.

This page intentionally left blank.

SECTION C - MODERN CRYPTOGRAPHY

Question 21. What is the KEY difference between classical and modern cryptography? [1 mark]

A. Classical cryptography focuses on all of the CIA properties, modern cryptography only focuses on confidentiality.

B. Classical cryptography is based on complex mathematical algorithms, modern cryptography is based on simple ciphers.

C. Classical cryptography security relies on secrecy of the algorithm, modern cryptography relies on the computational difficulty of solving a mathematical problem.

D. Classical cryptography is in widespread use in the digital world, modern cryptography is limited in its application.

Question 22. In symmetric encryption, how are encryption and decryption keys related? [1 mark]

A. They are the same key.

B. They are mathematically related but distinct.

C. They are completely unrelated.

D. Only the sender needs the encryption key.

Question 23. Which of the following is a common use case for a cryptographic hash? [1 mark]

A. Encrypting large volumes of data.

B. Securely exchanging keys over the internet.

C. Checking file integrity after download.

D. Transmitting messages confidentially.

Question 24. What is the MAIN role of Bob's public key used with PGP? [1 mark]

A. Decrypting messages sent by Bob

B. Encrypting messages intended for Bob

C. Signing messages to prove Bob's authorship

D. Securely exchanging symmetric keys

Question 25. How does a digital signature help ensure non-repudiation? [1 mark]

A. It encrypts the message content for confidentiality.

B. It allows anyone to verify the sender's identity.

C. It guarantees the message has not been modified.

D. It prevents the sender from copying the message.

Question 26. What is the MAIN advantage of RSA encryption? [1 mark]

A. Speed of encryption and decryption.
B. Algorithm has been kept secret.
C. Based on hard to solve problem - factoring large prime numbers.
D. Quantum resistance.

Question 27. Why might someone use BOTH symmetric and asymmetric encryption? [1 mark]

A. To double the encryption strength
B. To ensure both confidentiality and authenticity
C. To improve speed while maintaining key distribution advantages
D. Asymmetric encryption is always better, so this is unnecessary

Question 28. Which is a typical role of a Certificate Authority (CA)? [1 mark]

A. Stealing private keys to decrypt messages
B. Issuing digital certificates to verify public key ownership
C. Generating hash functions
D. Breaking encryption algorithms

Question 29. Which of the following is a potential weakness of the "Web of Trust" model used in systems like PGP? [1 mark]

A. Centralization and reliance on Certificate Authorities
B. Dependence on easily breakable symmetric cryptography
C. Difficulty in establishing trust for users outside your direct connections
D. Vulnerability to quantum computing attacks

Question 30. Which of the following is a KEY challenge to widespread adoption of post-quantum cryptography? [1 mark]

A. Existing classical computers cannot run these algorithms.
B. There are no known secure post-quantum algorithms.
C. Difficulty changing existing protocols to use post-quantum algorithms.
D. Quantum computers cannot run post-quantum algorithms.

SECTION D - AUTHENTICATION

Question 31. Which of these is NOT something an individual might use to authenticate themselves? [1 mark]

A. Something they are (biometrics)
B. Something they have (token)
C. Something they do (behavioral biometric)
D. Something they feel (emotional state)

Question 32. Offline password attacks are a concern because? [1 mark]

A. The attacker can take their time to crack the password file.
B. They are always successful.
C. They require no special tools.
D. The defender cannot detect the attack in real-time.

Question 33. Why is it ESSENTIAL to hash passwords rather than storing them in plain text? [1 mark]

A. Plain text passwords are too long to store efficiently.
B. Hashed passwords can be easily reversed to recover the original password.
C. Plain text passwords are vulnerable to data breaches, potentially exposing user credentials.
D. Hashed passwords take less processing power to verify.

Question 34. Using salted hashes for passwords is important because? [1 mark]

A. It lengthens the password.
B. It makes brute-force and rainbow table attacks significantly harder.
C. It guarantees passwords can never be cracked.
D. It allows users to recover forgotten passwords.

Question 35. A hardware token using a Time-based One-Time Password (TOTP) usually relies on? [1 mark]

A. A shared secret key and a synchronized clock
B. A network connection
C. A fingerprint scanner
D. A magnetic stripe reader

Question 36. What attack relies on multiple users using the same password on a single site to succeed? [1 mark]

A. Weak password.

B. Password spraying.

C. Credential stuffing.

D. Brute force.

Question 37. A biometric system reports a False Match Rate (FMR) of 1 in 1,000,000. What does this mean? [1 mark]

A. One in a million people will be incorrectly rejected.

B. There's a 1 in a million chance of the system malfunctioning.

C. One in a million attempts to spoof the system will succeed.

D. One in a million times, an unauthorized person will be granted access.

Question 38. You're designing a NEW authentication system where security is paramount. Which combination is likely MOST secure? [1 mark]

A. Password + fingerprint

B. Iris scan + voice recognition

C. PIN + hardware token (TOTP)

D. Password + SMS verification

Question 39. A website stores sensitive data. Users complain about forgotten passwords. You want to improve the situation while improving security. Which is LEAST likely to help? [1 mark]

A. Offering password hints

B. Using a hardware token

C. Allowing Single Sign-On (SSO) with trusted providers

D. Encouraging the use of password managers

Question 40. What is the PRIMARY advantage of a single sign-on (SSO) system? [1 mark]

A. It allows users to use one password across multiple related systems.

B. It eliminates the need for passwords entirely.

C. It increases the complexity of password creation requirements.

D. It reduces password fatigue for corporate employees.

SECTION E - MALWARE

Question 41. A piece of malware that secretly records your keystrokes and sends them to an attacker is known as? [1 mark]

A. Ransomware.
B. Keylogger.
C. Virus.
D. Trojan Horse.

Question 42. Boot sector viruses PRIMARILY infect? [1 mark]

A. Documents.
B. Master Boot Record on drives.
C. System backup files.
D. Website code.

Question 43. The technique where malware changes its appearance each time it spreads is called? [1 mark]

A. Metamorphic.
B. Signature-based.
C. Heuristic.
D. Polymorphic.

Question 44. A backdoor is a type of malware that? [1 mark]

A. Prevents access to your computer unless you pay.
B. Spreads by infecting executable files.
C. Collects and transmits browsing data.
D. Provides covert, unauthorized access to a system.

Question 45. Which of the following malware payloads likely has a financial motive? [1 mark]

A. Wiper.
B. Keylogger.
C. Ransomware.
D. Remote Access Trojan (RAT).

Question 46. A program disguises itself as a legitimate file but installs hidden malware when opened. This type of malware is which of the following? [1 mark]

A. Virus.

B. Trojan Horse.

C. Ransomware.

D. Worm.

Question 47. A virus attacks a system by appending itself to executable files. To avoid detection by an integrity checker, what other technique might it use? [1 mark]

A. Metamorphic obfuscation.

B. Encrypting its code.

C. Zero-day exploit.

D. Compression of executable files.

Question 48. Which of the following is a MAJOR weakness of signature-based anti-malware? [1 mark]

A. False negatives (flagging malware files as safe).

B. False positives (flagging safe files as malware).

C. Resource-intensive scanning.

D. Inability to detect unknown malware.

Question 49. An organization with highly sensitive data is choosing anti-malware settings. Which approach has the MOST significant potential downside? [1 mark]

A. Prioritizing strict detection rules, even if they lead to occasional false positives.

B. Setting detection to be less sensitive to reduce the disruption caused by false positives.

C. Focusing on behavioral analysis, accepting longer investigation time for alerts.

D. Employing a multi-layered security approach with only a single layer of anti-malware.

Question 50. Which of the following provides the STRONGEST support for the argument that "Perfect malware detection is impossible"? [1 mark]

A. Anti-malware systems can create false positives when scanning legitimate software.

B. New malware variants and techniques are constantly being developed.

C. Some malware is designed to remain hidden within memory without touching files.

D. Anti-malware signature updates always lag slightly behind new malware releases.

* * * * * * * * * * * * * * *