Mobile Security and Cryptography 101 Handout

Check Your Understanding Questions

Mobile Security

1. Why are smartphones such a high-value target for attackers?

   _____

2. Which of the following best describes the role of cryptography in mobile security?
   a. It prevents your phone from overheating.
   b. It helps improve battery life by optimizing app usage.
   c. It silently protects your data, identity, and communication.
   d. It speeds up your internet connection by compressing data.

   _____

Transposition Ciphers

1. Which of the following best describes how a transposition cipher works?
   a. It replaces each letter with a different letter or symbol.
   b. It scrambles the positions of characters without changing them.
   c. It hides the message using a numeric key.
   d. It converts plaintext into binary code.

   _____

Caesar and Classical Ciphers

1. If “FRGH” is the ciphertext of Caesar cipher using a shift of 3, what’s the original message?

   _____

2. Are classical ciphers difficult to break?

   _____

The Enigma Machine and Alan Turing

1. Why was the Enigma machine so hard to break during WWII?
   a. It used random numbers.
   b. It changed its settings every day.

c. It worked only in Morse code.
d. It was hidden underground.

_____

2. What made Alan Turing's approach to codebreaking different from earlier efforts?

_____

3. Is it hard to crack an encryption like the Enigma Machine using contemporary computation power?

_____

Asymmetric (Public Key) Encryption

1. What makes public key encryption different from classical encryption?
    a. Everyone shares one key.
    b. You use two different keys: one to encrypt and one to decrypt.
    c. The key changes every second.
    d. You don't need a key at all.

    _____

2. Put these steps in the correct order for sending a secure message:
    a. Alice encrypts a message.
    b. Bob sends Alice his public key.
    c. Bob uses his private key to decrypt it.

    _____

Cryptographic Handshake

1. Why is asymmetric (public key) encryption often used during the cryptographic handshake phase, even though symmetric encryption is more efficient?
    a. Because asymmetric encryption is faster.
    b. To securely exchange a shared private key for symmetric encryption.
    c. Because symmetric encryption doesn't work over the internet.
    d. To avoid using any keys at all.

    _____

2. In a typical cryptographic handshake, what happens after the shared key is securely exchanged?
    a. The connection is terminated.
    b. Public key encryption continues to be used for all communication.
    c. Symmetric encryption is used for the rest of the session.
    d. The shared key is discarded.

    _____

Modulo

1. What is 9 mod 4?

   _____

2. What is 23 mod 5?

   _____

RSA Cryptosystem

1. Match the following notations with their definition:

M	Plaintext message
C	Ciphertext message
e	Public exponent
d	Private exponent
n	Modulus (product of two primes)

   _____

2. What makes RSA an asymmetric (public key) cryptosystem?
   a. It's easy to lose your keys.
   b. It can only be used once.
   c. It's easy to encrypt using the public key, but hard to decrypt without the private key.
   d. It opens literal doors.

      _____

Cracking Modern Cryptosystem

1. If someone figures out how to factor large integers efficiently, does that mean they can break RSA and decrypt all our secrets?

   _____

Answer Key

Mobile Security

1. Smartphones store personal and sensitive data and are always connected, making them a valuable target.
2. c. It silently protects your data, identity, and communication.

Transposition Ciphers

1. b. It scrambles the positions of characters without changing them.

Caesar and Classical Ciphers

1. CODE
2. Once the method is known, they are easy to break.

The Enigma Machine and Alan Turing

1. b. It changed its settings every day.
2. He used mathematics, designed and used electromechanical machines (like the Bombe) to automate codebreaking.
3. No, modern computers can break it easily. A smartwatch has much more computation power than the massive Bombe machine.

Asymmetric (Public Key) Encryption

1. b. You use two different keys: one to encrypt and one to decrypt.
2. b, a, c

Cryptographic Handshake

1. b. To securely exchange a shared private key for symmetric encryption.
2. c. Symmetric encryption is used for the rest of the session.

Modulo

1. The answer is 1.
2. The answer is 3.

RSA Cryptosystem

1. M: Plaintext message
   C: Ciphertext message
   e: Public exponent
   d: Private exponent
   n: Modulus (product of two primes)
2. c. It's easy to encrypt using the public key, but hard to decrypt without the private key.

Cracking Modern Cryptosystem

1. Yes