Assignment 2

Course Number: SPR200
Course Name: Basic Cryptography
Course Section: NAA
Assignment Number: 2
Student Full Name: Zakariya Outbih
Student GitHub Username: zoutbih_seneca

Quiz 01, Question 01

Did you get it right in the quiz? Correct.
Question Statement: Please confirm that you understand this is a closed-book quiz, no aids can be used during the quiz. You cannot browse the internet, and you cannot browse any other content on BlackBoard except this quiz page. You understand the screen action of this quiz might be recorded in the lab.
Correct Answer: Yes, I confirm.
Why is the answer correct? This is a confirmation statement ensuring academic integrity. The correct answer acknowledges the rules and expectations for taking the quiz without external assistance.

Quiz 01, Question 02

Did you get it right in the quiz? Wrong.
Question Statement: What is the biggest difference between Theoretical Cryptography and Real-World Cryptography?
Correct Answer: Real-World Cryptography studies how to apply cryptography to solve problems.
Why is the answer correct? This is correct because Real-World Cryptography is concerned with practical applications and implementation, whereas Theoretical Cryptography emphasizes mathematical rigor and proof-based analysis.

Quiz 01, Question 03

Did you get it right in the quiz? Wrong.
Question Statement: "A cryptosystem should be secure even if everything about the system – except the key – is public knowledge."
Correct Answer: Kerckhoffs's Principle
Why is the answer correct? Kerckhoffs's Principle states that a cryptosystem must remain secure even when everything about the system is known publicly, except for the key. This principle promotes robustness and transparency in cryptographic system design.

Quiz 01, Question 04

Did you get it right in the quiz? Wrong.
Question Statement: Please write the LaTeX code for the equation: $F(x) = \left(\frac{x}{3}\right)^4\pi$
Correct Answer: `\(F(x) = \left(\frac{x}{3}\right)^4\pi\)`
Why is the answer correct? This LaTeX code uses `\frac` for the fraction, wraps it with parentheses using `\left( \right)`, raises it to the 4th power, and multiplies it by `\pi` — exactly matching the desired output.

Quiz 02, Question 01

Did you get it right in the quiz? Correct.
Question Statement: If a hash function has the property of collision resistance, then it must also have the property of second preimage resistance.
Correct Answer: True
Why is the answer correct? Collision resistance ensures it is difficult to find two different inputs that hash to the same output, which also implies second preimage resistance since you can't easily find a second input that hashes to the same output as a given one.

Quiz 02, Question 02

Did you get it right in the quiz? Correct.
Question Statement: Given a hash function and a digest of a preimage by the hash function, it is impossible to find out what the preimage is.
Correct Answer: False
Why is the answer correct? The preimage resistance depends on the design of the hash function. In some cases, depending on weaknesses or specific attacks, it may be possible to find the original input from the digest.

Quiz 02, Question 03

Did you get it right in the quiz? Incorrect.
Question Statement: What is the meaning of IV in the SHA512 diagram?
Correct Answer: Initialization Vector
Why is the answer correct? IV stands for Initialization Vector. It is used to initialize the internal state of the hash function to ensure uniqueness and randomness in the hashing process.

Quiz 03, Question 01

Did you get it right in the quiz? Correct.
Question Statement: What property in Group Theory is this graph demonstrating?
Correct Answer: Inverse element
Why is the answer correct? The graph demonstrates the inverse element property, which asserts that for each element in a group, there exists an inverse element such that their combination results in the identity element.

Quiz 03, Question 02

Did you get it right in the quiz? Correct.
Question Statement: We define the discrete logarithm problem with y = F(a,b,c), such that: `a = b^y (mod c) Please calculate: F(2, 3, 5) = 3`
Correct Answer: 3
Why is the answer correct? We are solving for y in the equation $2 = 3^y \mod 5$. If we plug in $y = 2$, we get $2 = 9 \mod 5$, which is 4, incorrect. If we plug in $y = 3$, we get $2 = 27 \mod 5$, which is 2. Therefore, the answer is 3.

Quiz 03, Question 03

Did you get it right in the quiz? Correct.
Question Statement: Same as Question 2, please calculate: F(1, 7, 10) = 4
Correct Answer: 4
Why is the answer correct? We are solving for y in the equation $1 = 7^y \mod 10$. If we plug in $y = 4$, we get $1 = 7^4 \mod 10$, which equals 2401 mod 10 = 1. Therefore, the answer is 4.

Quiz 03, Question 04

Did you get it right in the quiz? Correct.
Question Statement: [Ethical Question] Professor Feng is doing security research and using Tor browser to visit some anonymous websites set up in the Tor network. Suddenly, Professor Feng clicked some random link and before he realized it, a very graphical photo showed up below like this: [X]. In Professor Feng's best interest, what should he do (i.e., be safe and not get into trouble)?
Correct Answer: Immediately report to the authority with the link of the anonymous webpage on Tor network.
Why is the answer correct? The ethical and legal response is to immediately report the incident to the appropriate authorities to avoid any potential legal or personal issues. Handling such a situation properly can help protect both personal safety and compliance with the law. Also Mr. Wei would be very angry if you sent that to him.

Quiz 03, Question 05

Did you get it right in the quiz? Incorrect.
Question Statement: Diffie-Hellman Key Exchange is resilient to man-in-the-middle attack, because public keys `(g^a and g^b)` by Alice and Bob can be transmitted in an unsecured channel

anyway, so man-in-the-middle attack can't break Diffie-Hellman Key Exchange protocol.
Correct Answer: False
Why is the answer correct? The Diffie-Hellman key exchange is vulnerable to man-in-the-middle attacks because an attacker can intercept and modify the public keys exchanged between Alice and Bob, allowing them to establish a shared secret with each party. To prevent such attacks, additional authentication mechanisms are required.

Quiz 04, Question 01

Did you get it right in the quiz? Correct.
Question Statement: If you have a 10MB file, what could you NOT do with it?
Correct Answer: Using ECC private key to sign it.
Why is the answer correct? Signing a file with an ECC private key directly is not efficient for large files, as the signing process requires the file's hash to be computed and then signed. The other options (hashing, symmetric encryption after key exchange) are feasible with a 10MB file.

Quiz 04, Question 02

Did you get it right in the quiz? Incorrect.
Question Statement: ECC keys are generated in pairs, so the public key cannot be generated from the private key.
Correct Answer: False.
Why is the answer correct? ECC keys are generated in pairs: a private key and its corresponding public key. The public key can be derived from the private key using elliptic curve mathematics, so the statement that the public key cannot be generated from the private key is incorrect.

Quiz 04, Question 03

Did you get it right in the quiz? Incorrect.
Question Statement: ECC is efficient, and it runs faster for encryption than cryptographic hash functions like SHA3-512 generating the hash digest over the same file.
Correct Answer: False.
Why is the answer correct? ECC encryption is typically slower than hash functions like SHA3-512 for generating hash digests. Cryptographic hash functions are optimized for speed and efficiency, especially when applied to large files, while encryption operations in ECC require more computational resources.

Quiz 05, Question 01

Did you get it right in the quiz? Incorrect.
Question Statement: In the world of security, RSA refers to:
Correct Answer: All of the following: An asymmetric encryption primitive, A signature primitive, Three cryptographers' last name initials, A security company.
Why is the answer correct? RSA refers to the initials of Rivest, Shamir, and Adleman. It is used both as an asymmetric encryption and digital signature scheme. The algorithm is widely used in security protocols and is also the name of a security company.

Quiz 05, Question 02

Did you get it right in the quiz? Incorrect.
Question Statement: The following line: `public_key = private_key.public_key()` means that in RSA, a public key is generated from a private key in the RSA key generation algorithm.
Correct Answer: False.
Why is the answer correct? While the public key is mathematically derived from the private key's components, the key generation process produces both keys simultaneously. The method `private_key.public_key()` simply accesses the public part of the already-generated key pair.

Quiz 05, Question 03

Did you get it right in the quiz? Correct.
Question Statement: Match the following concepts.
Correct Answer:
1. Signing a digital signature using RSA: One's private key
2. Encrypt a message using ECC: One's public key
3. The maximum length of ECC encryption: Key size
4. PKCS#1 scheme: RSA padding

Why is the answer correct? Private keys are used to sign messages, and public keys to encrypt. ECC message length is constrained by key size. PKCS#1 defines padding for RSA encryption/signatures.

Quiz 05, Question 04

Did you get it right in the quiz? Incorrect.
Question Statement: The signature is generated by an Ed25519 private key directly from signing the message.
Correct Answer: False.
Why is the answer correct? Although Ed25519 private keys are used to sign messages, the signature internally involves hashing the message and other derived values—it's not a direct signature of the message like RSA might suggest.

Quiz 05, Question 05

Did you get it right in the quiz? Incorrect.
Question Statement: In Python, using `Ed25519PublicKey.verify()`, which of the following is NOT a required argument?
Correct Answer: Padding scheme and encoding.
Why is the answer correct? Ed25519 signatures do not require padding or encoding as arguments when verifying. Only the message and signature are necessary.

Quiz 06, Question 01

Did you get it right in the quiz? Incorrect.
Question Statement: For a ZKP protocol, if Alice wants to prove some x (witness) she knows of, while not revealing the value of x, she would need someone (Bob) to provide a challenge c, so she could continue with the proof and Bob can verify that Alice actually knows the value of x, according to the challenge c.
Correct Answer: False.
Why is the answer correct? In a Zero Knowledge Proof (ZKP), the prover (Alice) typically provides a proof that convinces the verifier (Bob) that she knows a secret value x, without revealing x. However, the challenge-response nature of the protocol often includes additional rounds or challenges, and not all ZKPs are based solely on a single challenge-response format.

Quiz 06, Question 02

Did you get it right in the quiz? Correct.
Question Statement: Match the following cryptographic concepts to their approximate appearance time in history.
Correct Answer:
1. Elliptic Curve: First
2. RSA Algorithm: Third
3. Digital Signature: Second
4. Zero Knowledge Proof: Fourth

Why is the answer correct? Elliptic curves are mathematical concepts documented throughout history, followed by the introduction of digital signatures. RSA was introduced in the late 1970s, and Zero Knowledge Proofs were introduced later as a concept in the 1980s.

Quiz 06, Question 03

Did you get it right in the quiz? Correct.
Question Statement: Select all the correct statements.
Correct Answer:
- In the interactive protocol of zero-knowledge proof, there is additional cost for the prover to prove that they have the witness.
- Using a ZKP protocol to generate a digital signature requires the use of a cryptographic hash function.
- Zero-knowledge proof can be used to prove Alice has some value x, but it cannot be used to prove that Alice has done some operations over x, e.g., Alice calculated $y = F(x)$.
- Creating a digital signature always requires a key in some form.

Why is the answer correct? ZKPs require interaction between the prover and verifier, and this incurs overhead. Digital signatures rely on cryptographic hash functions to ensure message integrity. ZKPs can prove knowledge of a value, but not the operations performed on it. Lastly, digital signatures require a private key for signing and a public key for verification.