UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab Quiz 5

Quiz relates to Lectures 13 and 14. Questions might have been seen in a different order on LEARN.

QUESTION 1

In the basic Diffie-Hellman key exchange protocol, Alice sends $A = g^a \mod p$ to Bob while Bob sends $B = g^b \mod p$ to Alice. In order to compute the shared secret, Bob computes:

(a) $A^b \mod p$

(b) $B^a \mod p$

(c) $Ag^b \mod p$

(d) $Bg^a \mod p$

$A^b \mod p$

QUESTION 2

Suppose that a cryptographic system uses both ECDSA and AES. If AES is implemented with 128-bit keys, to achieve a similar level of security, ECDSA should use elements of size:

(a) 160 bits

(b) 256 bits

(c) 384 bits

(d) 512 bits

---

256 bits

---

cont/...

QUESTION 3

ElGamal encryption in $\mathbb{Z}_p^*$ uses a modulus p, while RSA encryption uses a composite modulus n. When these are chosen to be of the same length:

(a) RSA ciphertexts and Elgamal ciphertexts are the same size

(b) RSA ciphertexts and Elgamal ciphertexts are of a random size

(c) RSA ciphertexts are twice the size of Elgamal ciphertexts

(d) Elgamal ciphertexts are twice the size of RSA ciphertexts

---

Elgamal ciphertexts are twice the size of RSA ciphertexts

QUESTION 4

The Diffie-Hellman protocol can be broken by an attacker who is able to:

(a) solve the discrete logarithm problem

(b) generate large prime numbers

(c) perform fast exponentiation

(d) observe previous runs of the protocol

---

solve the discrete logarithm problem

QUESTION 5

The Digital Signature Algorithm (DSA) is a standardised algorithm based on Elgamal signatures. Compared with RSA signatures at the same security level which of the following is true?

(a) DSA signatures are shorter than RSA signatures

(b) DSA signatures are more efficient to verify, even if the public RSA exponent equals 3

(c) DSA signatures cannot use elliptic curve groups but RSA signatures can

(d) DSA signatures do not require a random input but RSA signatures do

---

DSA signatures are shorter than RSA signatures

---

cont/...

QUESTION 6

When public key cryptography is used to provide digital signatures:

(a) the public key of the signer is required in order to generate the signature

(b) the public key of the verifier is required in order to generate the signature

(c) the private key of the signer is required in order to generate the signature

(d) the private key of the verifier is required in order to generate the signature

---

the private key of the signer is required in order to generate the signature

---

QUESTION 7

ECDSA is a standardised algorithm for digital signatures using elliptic curve groups. Which of the following statements about ECDSA is true?

(a) The ECDSA algorithm is believed to be secure against quantum computers

(b) ECDSA has shorter public keys than those for DSA signatures in $\mathbb{Z}_p^*$, for the same security level

(c) ECDSA signatures are larger than RSA signatures, for the same security level

(d) It is required that a different elliptic curve is generated for each user of ECDSA

ECDSA has shorter public keys than those for DSA signatures in $\mathbb{Z}_p^*$, for the same security level

---

QUESTION 8

A difference between a message authentication code (MAC) and a digital signature is:

(a) A digital signature scheme provides confidentiality but a MAC does not

(b) A digital signature scheme provides data integrity but a MAC does not

(c) A digital signature scheme provides non-repudiation but a MAC does not

(d) A digital signature scheme provides data authentication but a MAC does not

---

A digital signature scheme provides non-repudiation but a MAC does not

---

cont/...

QUESTION 9

In the ElGamal encryption scheme, a ciphertext for message m has two parts: $C_1 = g^k \mod p$ and $C_2 = m \cdot y^k \mod p$, where $y = g^x$ is the recipient public key. In order to recover the message, the recipient must compute:

(a) $C_1 \cdot (C_2^x)^{-1} \mod p$

(b) $C_2 \cdot (C_1^x)^{-1} \mod p$

(c) $C_1^x \cdot (C_2)^{-1} \mod p$

(d) $C_2^x \cdot (C_1)^{-1} \mod p$

$C_2 \cdot (C_1^x)^{-1} \mod p$

QUESTION 10

Three important computational problems in cryptography are: the discrete logarithm problem in Z_p^* (DLP), the discrete logarithm problem in elliptic curves (ECDLP) and the integer factorisation (IF) problem. If full-scale quantum computers become available then we know that:

(a) all three of these problems will have efficient solutions

(b) only IF will have an efficient solution

(c) only DLP will have an efficient solution

(d) only IF and DLP will have efficient solutions

---

all three of these problems will have efficient solutions
