UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab Quiz 2

Quiz relates to Lectures 7 and 8. Questions might have been seen in a different order on LEARN.

QUESTION 1

In an iterative block cipher, the purpose of the key schedule is to:

(a) define how to derive the round keys from the master key

(b) generate different keys for every block encrypted

(c) choose between different master keys

(d) define how the master key is generated

---

define how to derive the round keys from the master key

QUESTION 2

The Data Encryption Standard (DES) is an iterated block cipher. In each round the DES algorithm:

(a) performs a substitution on a complete block

(b) operates on multiple blocks at the same time

(c) performs a non-linear operation

(d) uses the same key bits

---

performs a non-linear operation

---

cont/...

QUESTION 3

Which of the following encryption algorithms has the largest number of possible keys?

(a) DES (the Data Encryption Standard algorithm)

(b) The random simple substitution cipher on an alphabet of 26 characters

(c) A transposition cipher on blocks of size 10

(d) The Vigenere cipher with a key of length 5 and an alphabet of 26 characters

---

The random simple substitution cipher on an alphabet of 26 characters

---

QUESTION 4

Double encryption with DES (double DES) with two independent keys:

(a) has twice as many possible key values as ordinary DES

(b) uses half as much computation as ordinary DES

(c) runs twice as fast as ordinary DES

(d) is vulnerable to a meet-in-the-middle attack

---

is vulnerable to a meet-in-the-middle attack

QUESTION 5

Triple DES is a variant of the original Data Encryption Standard (DES) algorithm. In Triple DES:

(a) the original DES algorithm is run three times for each input block

(b) the block size is three times longer than original DES

(c) the algorithm runs three times faster than original DES

(d) there are three times as many possible keys as original DES

---

the original DES algorithm is run three times for each input block

---

cont/...

QUESTION 6

AES, the Advanced Encryption Standard, algorithm:

(a) has a 128 bit block size

(b) has a 192 bit block size

(c) has a 256 bit block size

(d) allows any of the other block sizes

has a 128 bit block size

QUESTION 7

Each round of the AES algorithm:

(a) performs a substitution on a complete block

(b) operates on multiple blocks at the same time

(c) performs a non-linear operation

(d) uses the same key bits

performs a non-linear operation

QUESTION 8

Which of the following modes of operation for block ciphers does not introduce randomness?

(a) CBC mode

(b) CTR mode

(c) ECB mode

(d) OFB mode

ECB mode

QUESTION 9

Counter mode (CTR) is a mode of operation for block ciphers. Which of the following statements about CTR mode is true?

(a) Messages to be encrypted must be padded to be a complete number of blocks

(b) One bit in error in the ciphertext leads to a whole random block in the decrypted plaintext

(c) Equal plaintext blocks encrypt to equal ciphertext blocks

(d) Decryption of a sequence of blocks can be conducted in parallel

---

Decryption of a sequence of blocks can be conducted in parallel

---

QUESTION 10

The main disadvantage of basic Electronic Code Book (ECB) mode of operation for block ciphers, in comparison with counter mode (CTR) and cipher block chaining (CBC) mode, is:

(a) ECB mode encryption is less efficient

(b) ECB mode has large error propagation

(c) equal plaintext blocks in ECB mode give equal ciphertext blocks

(d) ECB mode requires longer keys

---

equal plaintext blocks in ECB mode give equal ciphertext blocks

---

UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab Quiz 1

Quiz relates to Lectures 3, 5 and 6. Questions might have been seen in a different order on LEARN.

QUESTION 1

The inverse of 3 modulo 17 is:

(a) 4

(b) 1

(c) 3

(d) 6

6

QUESTION 2

Which of the following integers does not have an inverse modulo 21?

(a) 1

(b) 2

(c) 3

(d) 4

3

QUESTION 3

Which of the following integers is a generator for $\mathbb{Z}_7^*$, the non-zero integers modulo 7?

(a) 1

(b) 2

(c) 3

(d) 6

3

QUESTION 4

What is $8^{-1} \mod 21$?

(a) 1

(b) 2

(c) 4

(d) 8

8

QUESTION 5

A generator for $\mathbb{Z}_{15}^*$ has order:

(a) 1

(b) 3

(c) 8

(d) 14

8

QUESTION 6

Which of the following is a fundamental weakness of the Hill cipher for any size of encryption matrix?

(a) The number of possible keys is too small

(b) Encryption is a linear function

(c) The encryption function is computationally expensive

(d) Decryption is not always possible

Encryption is a linear function

QUESTION 7

Following Kerckhoff's principle, we usually assume that an attacker of an encryption scheme has access to:

(a) unbounded computational power

(b) the encryption and decryption keys

(c) the description of the encryption and decryption algorithms

(d) all of the above

the description of the encryption and decryption algorithms

QUESTION 8

If a plaintext comes from a natural language, such as English, which of the following encryption algorithms can be expected to have the most uniform ("flattest") frequency distribution of ciphertext characters?

(a) The Caesar cipher

(b) The random simple substitution cipher

(c) A transposition cipher on blocks of size 12

(d) The Vigenere cipher with a key of length 8

The Vigenere cipher with a key of length 8

cont/...

QUESTION 9

If a plaintext comes from a natural language, such as English, for which of the following ciphers is the frequency of any particular character equal in both plaintext and ciphertext?

(a) The Caesar cipher

(b) The random simple substitution cipher

(c) A transposition cipher on blocks of size 12

(d) The Vigenere cipher with a key of length 8

A transposition cipher on blocks of size 12

QUESTION 10

Which is the smallest of the following key sizes that would be acceptable to prevent exhaustive key search today?

(a) 256 bits

(b) 512 bits

(c) 1024 bits

(d) 2048 bits

256 bits

UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab Quiz 4

Quiz relates to Lectures 11 and 12. Questions might have been seen in a different order on LEARN.

QUESTION 1

The Merkle-Damgård construction for hash functions makes use of a compression function, h, which acts on successive message blocks. A benefit of this construction is:

(a) computation of a hash value requires a fixed number of calls to h, independent of the length of the input message

(b) if h is collision-resistant then the whole hash function is collision-resistant

(c) no padding is required for the input message, no matter what is the output size of h

(d) the length of the input message does not need to be included

---

if h is collision-resistant then the whole hash function is collision-resistant

---

QUESTION 2

Due to the birthday paradox, we can expect to find a collision in the SHA-256 hash function after around:

(a) 2^7 trials

(b) 2^8 trials

(c) 2^{128} trials

(d) 2^{255} trials

2^{128} trials

QUESTION 3

Suppose that an attacker has the ability to compute the output of a certain hash function for 2^{128} input values. In order to prevent the attacker from finding a collision in the hash function, the output of the hash function should be of length at least:

(a) 128 bits

(b) 256 bits

(c) 384 bits

(d) 512 bits

---

384 bits

QUESTION 4

A message authentication code (MAC) takes as input a message and a key and outputs a tag. To be considered secure a MAC should have the property:

(a) the correct tag for a new message cannot be computed without the key

(b) the message used to compute the tag cannot be distinguished from a random message

(c) different tags are computed if a message is repeated

(d) any output tag cannot be distinguished from a random string

---

the correct tag for a new message cannot be computed without the key

---

QUESTION 5

Which of the following block cipher modes of operation is not designed to provide data confidentiality?

(a) Counter mode (CTR)

(b) Cipher block chaining (CBC)

(c) Cipher-based MAC (CMAC)

(d) Counter with CBC-MAC (CCM)

Cipher-based MAC (CMAC)

QUESTION 6

Which of the following block cipher modes of operation is not designed to provide data integrity?

(a) Galois counter mode (GCM)

(b) Cipher block chaining (CBC)

(c) Cipher-based MAC (CMAC)

(d) Counter with CBC-MAC (CCM)

Cipher block chaining (CBC)

QUESTION 7

When public key cryptography is used for encryption:

(a) the public key of the sender is required in order to decrypt the ciphertext

(b) the public key of the receiver is required in order to decrypt the ciphertext

(c) the private key of the sender is required in order to decrypt the ciphertext

(d) the private key of the receiver is required in order to decrypt the ciphertext

the private key of the receiver is required in order to decrypt the ciphertext

QUESTION 8

The keys for the RSA encryption algorithm include a public exponent e, a private exponent d, and a public modulus n. It is common to choose:

(a) $d = 2^{16} + 1$

(b) $e = 2^{16} + 1$

(c) $e = n - 1$

(d) $d = n - 1$

$e = 2^{16} + 1$

QUESTION 9

For the RSA encryption scheme a large modulus n is chosen, typically around 2048 bits in practice. To improve efficiency, this is often used together with:

(a) a small value for e

(b) a small value for d

(c) a small value for one of the factors of n

(d) a small value for the Euler function $\phi(n)$

---

a small value for e

QUESTION 10

For any given values x and m, the square-and-multiply algorithm when used to compute $x^{66} \mod m$ requires:

(a) 5 squarings and 3 multiplications modulo m

(b) 6 squarings and 1 multiplication modulo m

(c) 8 squarings and 1 multiplication modulo m

(d) 63 squarings and 3 multiplication modulo m

---

6 squarings and 1 multiplication modulo m

UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab Quiz 6

Quiz relates to Lectures 15 and 16. Questions might have been seen in a different order on LEARN.

QUESTION 1

Digital certificates are signed by a certification authority. In order to make certificate verification as fast as possible, it is common for this purpose to use:

(a) RSA signatures

(b) Elgamal signatures

(c) DSA signatures

(d) ECDSA signatures

RSA signatures

QUESTION 2

An alternative to a hierarchical PKI is to use *web of trust*. An important property in a web of trust, that does not apply in a hierarchical PKI, is that:

(a) private keys can be generated by any party

(b) public keys can be signed by any party

(c) subjects can remain anonymous

(d) a variety of different signature algorithms can be used to sign certificates

---

public keys can be signed by any party

QUESTION 3

Two commonly used digital signatures schemes are RSA signatures and ECDSA. RSA is commonly used to sign digital certificates. This is because, for the same security level:

(a) RSA public key lengths are shorter

(b) RSA signatures are shorter

(c) RSA signature generation is faster

(d) RSA signature verification is faster

RSA signature verification is faster

QUESTION 4

In order to produce a digital certificate, a certification authority computes:

(a) an encryption of the subject's private key and identity

(b) an encryption of the subject's public key and identity

(c) a signature on the subject's private key and identity

(d) a signature on the subject's public key and identity

a signature on the subject's public key and identity

QUESTION 5

An X.509 digital certificate is issued by a certification authority. In order to verify such a certificate it is necessary, in addition to the certificate itself, to have:

(a) the subject's private key

(b) the subject's public key

(c) the certification authority's private key

(d) the certification authority's public key

the certification authority's public key

cont/...

QUESTION 6

The original Needham-Schroeder protocol is known to be vulnerable to a replay attack. This means that:

(a) an honest party accepts a session key used in a previous run of the protocol

(b) an honest party re-uses its nonce used in a previous run of the protocol

(c) the attacker obtains the long-term key of an honest party

(d) the attacker obtains the nonce used by an honest party

---

an honest party accepts a session key used in a previous run of the protocol

---

QUESTION 7

The basic ephemeral Diffie–Hellman protocol can be strengthened by adding to each message a digital signature of the sender. The effect of this on the protocol is to:

(a) provide entity authentication

(b) allow shorter Diffie–Hellman parameters

(c) prevent replay attacks

(d) prevent attacks which can find discrete logarithms

---

provide entity authentication

QUESTION 8

Forward secrecy is the property that:

(a) if a user's long term key becomes known to an attacker, session keys established earlier are not compromised

(b) if a user's long term key becomes known to an attacker, session keys established later are not compromised

(c) if a user's session key becomes known to an attacker, that user's long term key is not compromised

(d) if a user's session key becomes known to an attacker, that user's long term key is also compromised

---

if a user's long term key becomes known to an attacker, session keys established earlier are not compromised

---

cont/...

QUESTION 9

The basic ephemeral Diffie-Hellman protocol can be authenticated by adding to each message a digital signature of the sender. The protocol then provides forward secrecy because:

(a) revealing the Diffie-Hellman shared secret does not reveal the signing keys

(b) revealing the signing keys does not reveal the Diffie-Hellman shared secret

(c) revealing the Diffie-Hellman ephemeral secret keys does not reveal the Diffie-Hellman shared secret

(d) revealing the Diffie-Hellman ephemeral secret keys does not reveal the signing keys

revealing the signing keys does not reveal the Diffie-Hellman shared secret

QUESTION 10

When assessing the security of a key establishment protocol such as the Needham-Schroeder protocol, we assume that an attacker is able to:

(a) obtain any session keys used in previous runs of the protocol

(b) obtain the long-term key of the parties involved in the protocol run under attack

(c) break any encryption algorithm used in the protocol

(d) force any protocol participant to repeat nonce values

obtain any session keys used in previous runs of the protocol

UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2020

Lab Quiz 7

Quiz relates to Lectures 17 and 18. Questions might have been seen in a different order on LEARN.

QUESTION 1

The purpose of the record protocol in TLS is to:

(a) change the cryptographic algorithms from previously used ones
(b) signal events such as failures
(c) set up sessions with the correct keys and algorithms
(d) provide confidentiality and integrity for messages

---

provide confidentiality and integrity for messages

QUESTION 2

The purpose of the handshake protocol in TLS is to:

(a) change the cryptographic algorithms from previously used ones
(b) signal events such as failures
(c) set up sessions with the correct keys and algorithms
(d) provide confidentiality and integrity for application messages

---

set up sessions with the correct keys and algorithms

QUESTION 3

When TLS is used to protect web browser communications with HTTPS, a man-in-the-middle (MITM) attack is possible if an attacker is able to:

(a) masquerade as a network node

(b) add root certificates into the browser

(c) obtain a valid server certificate

(d) alter the hello messages in the TLS handshake

add root certificates into the browser

QUESTION 4

Let us consider the following TLS cipher suite: `TLS_RSA_WITH_AES_128_CBC_SHA`. When this cipher suite is chosen, RSA is used:

(a) to sign the server's ephemeral Diffie-Hellman value

(b) to sign the client's ephemeral Diffie-Hellman value

(c) to encrypt the pre-master secret with the server's long-term key

(d) to encrypt the pre-master secret with the client's long-term key

to encrypt the pre-master secret with the server's long-term key

QUESTION 5

Galois counter mode (GCM) is often used in TLS to provide:

(a) data confidentiality

(b) data integrity

(c) error checking

(d) authenticated encryption

authenticated encryption

cont/...

QUESTION 6

How is the ciphersuite used in a run of the TLS protocol decided?

(a) It is chosen by the server

(b) It is chosen by the client

(c) It is negotiated between client and server

(d) It is defined by the latest version of TLS

It is negotiated between client and server

QUESTION 7

Which of the following features is not available in TLS 1.3?

(a) Authenticated encryption with associated data

(b) Forward secrecy

(c) Stream ciphersuite

(d) Data compression

Data compression

QUESTION 8

The TLS 1.3 handshake protocol is NOT concerned with:

(a) Session key renewal

(b) Session key confirmation

(c) Public key certificates

(d) Cipher suite renegotiation

Cipher suite renegotiation

QUESTION 9

When TLS uses authenticated encryption modes, such as CCM or GCM, the additional authenticated data includes:

(a) the session key

(b) the pre-master secret

(c) the peer certificate

(d) the sequence number and header data

---

the sequence number and header data

QUESTION 10

A construction for a message authentication code from any hash function, often used in TLS, is known as:

(a) CMAC

(b) HMAC

(c) SHA-1

(d) GCM

HMAC

UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab Quiz 3

Quiz relates to Lectures 9 and 10. Questions might have been seen in a different order on LEARN.

QUESTION 1

Which of the following is not a binary synchronous stream cipher?

(a) the one time pad

(b) RC4

(c) SHA-1

(d) A5/1

SHA-1

QUESTION 2

In a binary synchronous stream cipher:

(a) the keystreams generated by the sender and receiver are the same

(b) the keystreams generated by the sender and receiver are complementary (every bit is different)

(c) the keystream generated by the receiver is the XOR sum of the plaintext and the keystream generated by the sender

(d) the keystream generated by the receiver is the XOR sum of the ciphertext and the keystream generated by the sender

---

the keystreams generated by the sender and receiver are the same

---

QUESTION 3

The one time pad:

(a) provides data integrity
(b) provides perfect secrecy
(c) produces ciphertext which is twice the length of the plaintext
(d) requires much more computation for encryption than for decryption

provides perfect secrecy

QUESTION 4

Which of these statements about the keystream used in the one time pad is true?

(a) The keystream has a large, but finite, period
(b) The keystream starts with an initialisation vector (IV)
(c) The keystream is generated by a linear feedback shift register (LFSR)
(d) Each keystream bit is only used once

Each keystream bit is only used once

QUESTION 5

In typical usage, a true random number generator (TRNG) and a pseudo-random number generator (PRNG) are often combined in practice so that:

(a) the PRNG provides the seed for the TRNG
(b) the TRNG provides the seed for the PRNG
(c) the TRNG and the PRNG output alternate bits
(d) the TRNG and PRNG output is combined using exclusive-OR (XOR)

the TRNG provides the seed for the PRNG

cont/...

QUESTION 6

The Fermat test can be used to decide whether or not a number n is prime. The test can sometimes fail with the result that:

(a) a prime number is labelled as a composite number

(b) a composite number is labelled as a prime number

(c) the test halts without producing any output

(d) the test continues computing without producing a result

a composite number is labelled as a prime number

QUESTION 7

By Euler's theorem, if $\gcd(a, n) = 1$ then it is always true that:

(a) $a^{n-1} \mod \phi(n) = 1$

(b) $a^{n-1} \mod n = 1$

(c) $a^{\phi(n)} \mod \phi(n) = 1$

(d) $a^{\phi(n)} \mod n = 1$

$a^{\phi(n)} \mod n = 1$

QUESTION 8

Which of the following pairs of equations cannot be solved using the Chinese Remainder Theorem?

(a) $x \equiv 3 \mod 5$ and $x \equiv 3 \mod 11$

(b) $x \equiv 3 \mod 6$ and $x \equiv 4 \mod 11$

(c) $x \equiv 3 \mod 5$ and $x \equiv 3 \mod 12$

(d) $x \equiv 3 \mod 6$ and $x \equiv 4 \mod 12$

$x \equiv 3 \mod 6$ and $x \equiv 4 \mod 12$

QUESTION 9

Suppose $n = 77 = 7 \times 11$. According to Euler's theorem:

(a) $2^7 \mod n = 1$

(b) $2^{11} \mod n = 1$

(c) $2^{60} \mod n = 1$

(d) $2^{76} \mod n = 1$

$2^{60} \mod n = 1$

QUESTION 10

Let g be a generator for the integers modulo p. The discrete logarithm problem is:

(a) given y, find x with $y = x^g \mod p$

(b) given x, find y with $y = x^g \mod p$

(c) given y, find x with $y = g^x \mod p$

(d) given x, find y with $y = g^x \mod p$

---

given y, find x with $y = g^x \mod p$

UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab Quiz 8

Quiz relates to Lectures 19 and 20. Questions might have been seen in a different order on LEARN.

QUESTION 1

A difference between the public key infrastructure used by TLS for web browsers, and that provided by PGP for email security, is:

(a) PGP keys can be signed by any other user

(b) PGP keys are certified in a hierarchical manner

(c) PGP keys have no expiry date

(d) PGP keys can use any type of public key algorithm

PGP keys can be signed by any other user

QUESTION 2

PGP is a security protocol to protect emails in transit. Which of the following statements about PGP is true:

(a) it provides confidentiality of metadata such as email headers

(b) it provides end-to-end security between the sender and recipient

(c) it requires special processing by email servers during email transit

(d) it uses hierarchical digital certificates as also used in HTTPS

---

it provides end-to-end security between the sender and recipient

---

QUESTION 3

STARTTLS is a security protocol often used to protect emails in transit. For this purpose:

(a) STARTTLS can provide only client-server security

(b) STARTTLS can provide client privacy

(c) STARTTLS can provide only link-by-link security

(d) STARTTLS can provide client end-to-end security

STARTTLS can provide only link-by-link security

QUESTION 4

STARTTLS is a security protocol often used to protect emails in transit. When used for email protection, STARTTLS:

(a) can protect confidentiality of email contents from malicious mail servers

(b) can provide end-to-end security between the sender and recipient

(c) requires special processing by email clients

(d) can apply cryptographic protection to metadata such as email headers

can apply cryptographic protection to metadata such as email headers

QUESTION 5

One common way to apply the IPsec protocol uses a gateway-to-gateway architecture. Which of the following statements about this architecture is true?

(a) It is typically used to provide secure remote access from a single host

(b) It is typically used for secure remote management of a single server

(c) It provides protection for data throughout its transit (end-to-end)

(d) It is typically used with IPsec in tunnel mode

It is typically used with IPsec in tunnel mode

QUESTION 6

One common way to apply the IPsec protocol uses a host-to-host architecture. Which of the following statements about this architecture is true?

(a) It is often used to connect hosts on unsecured networks to resources on secured networks

(b) A typical application is to securely connect two separate secure networks

(c) It provides protection for data throughout its transit (end-to-end)

(d) It is typically used with IPsec in tunnel mode

It provides protection for data throughout its transit (end-to-end)

QUESTION 7

Like TLS, IPSec can be used to set up secure communication between nodes. Which of the following applies to IPSec, but not to TLS?

(a) Different suites of cryptographic algorithms can be used.

(b) Traffic flow confidentiality may be provided.

(c) Forward secrecy may be provided using Diffie-Hellman key exchange.

(d) The protocol specification defines both key establishment and security of user data.

Traffic flow confidentiality may be provided.

QUESTION 8

Transport mode is generally used in:

(a) host-to-host architectures

(b) gateway-to-gateway architectures

(c) host-to-gateway architectures

(d) gateway-to-host architectures

---

host-to-host architectures

---

cont/...

QUESTION 9

POP and IMAP are mail access protocols to let:

(a) a MUA download an email from a MTA.

(b) a MUA upload an email to a MTA.

(c) a MTA download an email from a MUA.

(d) a MTA upload an email to a MUA.

---

a MUA download an email from a MTA.

QUESTION 10

DKIM is:

(a) a specification for cryptographically signing email messages.

(b) a policy-based specification describing how emails should be handled.

(c) a protocol to allow X.509 certificates to be bound to DNS names.

(d) a directory lookup service providing a maaping between host name and IP address.

---

a specification for cryptographically signing email messages.

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

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
