*Which of the following is* ***not*** *true of X.509 certificates?*

X.509 certificates specify public standards for public key certificates

An X.509 certificate uniquely identifies a subject

An X.509 certificate specifies a subject's public key

An X.509 standard is signed in plain text

An X.509 certificate should be validated. Which of the following is not necessary?

Obtain the public key of the issuer of the certificate

Decipher the signature on the certificate using the CA's private key

Ensure that the certificate is current

Decipher the signature on the certificate using the CA's public key

User authentication

Establishes what IT system assets a user has access to

Establishes the identity of IT system users

Describes what operations a user may perform on data

Verifies that a user's IT system account is secure

Imagine a system which uses an 8-character password composed of only the 26 lower case letters (a..z). An attacker has an automated system that can test 100 passwords per second, There is no delay after a failed login and no maximum number of attempts, Using Anderson’s formula (slide 20 unit 3.1). What is the probability of discovering the correct password within a year (365 days)?

Between 0 and 0.05

Between 0.05 and 0.5

Between 0.5 and 0.95

Between 0.95 and 1

Which of the following is not a plausible disadvantage of a biometric authentication system?

A person's biometrics are not as unique as the passwords they could choose

Assessing biometrics is slower than checking password hashes

Matches are not exact: an acceptable balance of false positives and false matches needs to be determined

Systems for comparing biometrics are not accurate enough

Some authorities recommend the use of three random words as a password/passphrase (eg ‘giraffe songmaker weather’). Which of the following is a potential weakness of such passwords?

They may be easier for users to remember

They may be naturally relatively longer than ‘traditional’ complex passwords

Users are less likely to write them down

They are dictionary words

System admins (sysadmins) at Egg bank used a challenge-response system to connect to the bank’s IT system. Each administrator had a security token which displayed a unique number, changing each minute, which must be correctly entered on login. One advantage of such a system is:

The sysadmin no longer needs to remember a password

An attacker is likely to be able to guess the unique number at any given time

It guards against the system administrator's password being compromised

A number is harder to guess because it's not a dictionary word

Using a bank card to extract money from an ATM is an example of which of the following?

Authentication using what the user knows

Authentication using what the user has

Authentication using where the user is

Two-factor authentication

A salt is a?

Randomly-generated string added to a password after hashing

Randomly-generated string added to a password before hashing

Method to ensure users choose long complex passwords

Password encryption method

The index of coincidence gives

The probability that two randomly chosen letters from ciphertext will be the same

The frequency of a given letter in a language

The correlation frequency between the same letter in a ciphertext and a language

The probability that the ciphertext was generated using a random key

Public key infrastructure (PKI) enables which of the following?

Public keys to be distributed without being lost in transit

People, systems And organisations to trust each other's private keys

People, systems and organisations to trust each other's public keys

Certification authorities to control communication

Secure shell (ssh) is an example of a network protocol which uses public-key cryptography between servers. Which is TRUE

ssh ensures availability of the servers

ssh ensures confidentiality and integrity of data transmitted between servers

Ssh cannot detect a man-in-the-middle attack

ssh enforces checking of keys with a Certification Authority

A root certification authority

Must keep its public key secure

Is the ultimate arbiter of trust for public keys used within a community (e.g. a company)

Secures administrative access to a server

Must have its public key signed by a higher-level authority

Suppose that Eve successfully conducts a man-in-the-middle attack between Alice and Bob. Which of these statements is then **not** true?

Eve intercepts communications between Alice and Bob

Eve impersonates Alice and Bob in their (no longer) secret communication with each other

Eve sends Bob and Alice her own public key

Alice and Bob can detect Eve by carefully inspecting the keys and messages which they receive

In a password-protected access system, complementary information is?

Information stored on computer used to validate the password

Information an attacker obtains to help determine a user's password

A login success message

The function which checks the validity of the user's password

CAPTCHA (for example where a website asks you to click all pictures in a grid which contain part of a car) is a

Strong password

Challenge-response authentication

Salt

Encryption key

If Bob sends a message to Alice, Bob should encrypt the message with his private key so that

Alice can be sure that Bob sent the message

The message cannot be decrypted by anyone other than Alice

Alice can respond to the message securely

Bob can later deny that he sent the message

Charlie obtains some information about Sarah based on her publicly available social media. He guesses her email address based on her name and guesses her password based on the information he has discovered when he uses this email / password combination to attempt to log into the Fastshop.com website, the website refuses his access and displays the message “password incorrect”. This is a security breach because of which of the following?

The account has not been locked, he is free to try a new password

He can now be relatively sure that that the email address is correct and concentrate on guessing the password

He now knows that his guessed password was not complex enough

It is not a security breach

Which of the following is true of hash functions and hashes (checksums)?

A hash should be at least as long as the message

A hash should be hard to compute

It should be infeasible to generate a message corresponding to a given hash

It should be relatively simple to find two messages having the same hash

The index of coincidence is useful for:

Spotting repeated patterns in the ciphertext

Determining the likely length of the key used for encryption

Generating secure session keys

Determining whether a session key has been compromised