In order to be issued an SSL Certificate, you need to purchase one from a web service provider and then go through a process that entails the following:

Purchasing SSL – Place an order for an SS…

Private Key and CSR Generation – Prior to applying/enrolling…

Private Key and CSR Generation – Digital IDs make use of a…

Private Key and CSR Generation – The Private Key will rem…

Private Key and CSR Generation – hosting server will gener…

Enrollment – Generated a minimum o…

Enrollment – This process is done from…

Enrollment – The contact details that y…

Verification Process & Certificate Issue – After submitting the requ…

Verification Process & Certificate Issue – This process is much fas…

Verification Process & Certificate Issue – After the CA is satisfied w…

Verification Process & Certificate Issue – After you have done the…

Identify the following prime numbers. choose all that apply.

751, **347**, **491**, **421**, **491**,**19**

Process of converting electronic data into another form, called cipher text, which cannot be easily understood by anyone except the authorized parties. This assures data security.

Encryption

Type of cryptography also known as public-key cryptography. It uses public and private keys to encrypt and decrypt data.

Digital Certificate

These are whole numbers greater than 1 whose only factors are 1 and itself. A factor is a whole number that can be divided evenly into another number.

Prime number

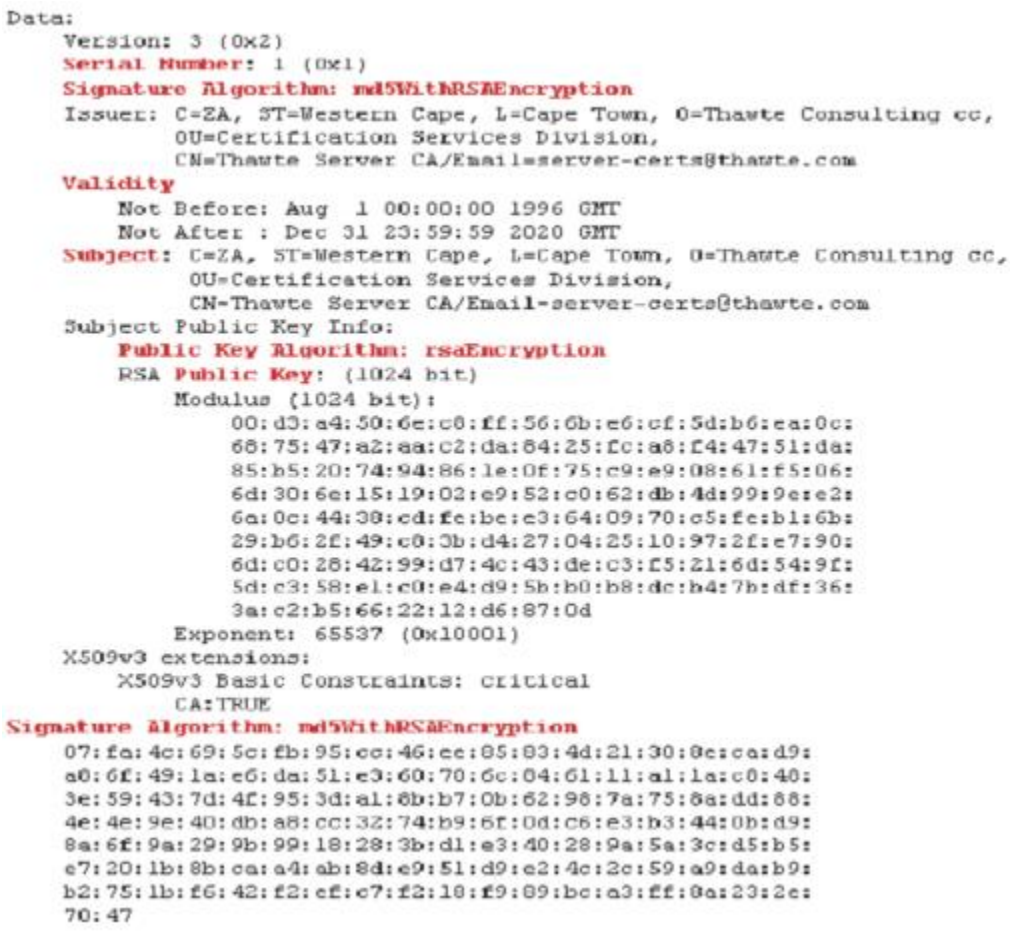
What type of encryption that the sender and receiver use different keys (aka two-key, and public-key)?

Asymmetric

It is the process of attempting to discover the plain text or the key of an encrypted file.

Cryptanalysis

Base on the figure below, this is an example of a _____?



RSA

public key

A type of cryptography that uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical. One key in the pair

can be shared with everyone; it is called the public key, while the other key serves as the private key used to decipher the encrypted data.

Asymmetric cipher

It is the assurance that someone cannot deny the validity of something. It is also a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data.

Non-repudiation

It is a widely accepted type of digital certificated by international public key infrastructure standards to verify that a public key belongs to the user, computer, or service identity contained within the certificate.

x.509

It is a cryptographic algorithm that can be used to protect electronic data, its main strength rests in the option for various key lengths, a 128-bit, 192-bit or 256-bit key, the algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

Advance encryption standard

Identify the different types of Digital Certificates by Matching Column A with Column B

Server Certificates – Allows visitors to exchan…

Server Certificates – are used by corporate en…

Personal Certificates – Prove authorship and re…

Personal Certificates – These are perfect for bus…

Corporate Certificates – Client Certificates or Dig…

Corporate Certificates – These are perfect for bus…

Developer Certificates – Prove authorship and ret…

Developer Certificates – Used to sign software or…

Identify the 2 different types of SSL Certificates by Matching Column A with Column.

Basic SSL certificate – It allows you to secure o…

Basic SSL certificate – This certificate is quite w…

Basic SSL certificate – If you want to also anoth…

Wildcard SSL certificate – allows you to secure you…

Wildcard SSL certificate – This is best suited for lar…

Which of the following are the basic SSL Certificates? Choose all that applies.

SSL 123, Positive SSL

What are the 2 things does SSL Certificates do?

Authenticate your website's identity.

Encrypt the information sent from your website visitor's browser to your website

What are the 3 Popular Forms of Encryption? answer in lowercase only

Aes, des, rsa

It is an electronic attachment document used for security purposes that is used to identify an individual, a server, a company, or some other entity, and to associate that identity with a public key.

Digital certificate

It is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. Its purpose is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

public key infrastructure

It is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It guarantees that the contents of a message have not been altered in transit.

digital signature

It is a cryptographic algorithm that can be used to protect electronic data, its main strength rests in the option for various key lengths, a 128-bit, 192-bit or 256-bit key, the algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

advance encryption standard

The oldest and most used cryptographic ciphers, the key that deciphers the cipher text is the same key enciphers the plaint text, this key is often referred to as the secret key.

symmetric cipher

It is a pioneering encryption algorithm that helped revolutionize encryption, it is symmetric type encryption method developed in 1975 and standardized by ANSI in 1981 as ANSI X. It uses 56 bit and 48 bit key and 64 bit block cipher.

data encryption standard

A type of cryptography that uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical. One key in the pair can be shared with everyone; it is called the public key, while the other key serves as the private key used to decipher the encrypted data.

asymmetric cipher

It is one of the first public-key cryptosystems and is widely used for secure data transmission, in such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret or private. It is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

rsa

These are number of positive integers that are relatively prime to (or do not contain any factor in common with the given numbers) and where 1 is counted as being relatively prime to all numbers.

totient

Write the formula of the euler's function: totient = ?

(p-1)*(q-1)

It is an art and science of transforming messages so as to make them secure and immune to attacks.

cryptography

What are the two basic principles of encryption? answer in lowercase only

substitution, transposition

What type of encryption that the sender and receiver use the same key (aka single-key, and secret-key)?

symmetric

What type of encryption that the sender and receiver use different keys (aka two-key, and public-key)?

asymmetric

Type of encryption processing that processes the input in a block of elements at a time (typically 64-bits)?

Block cipher

It is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.

Worm

It is any malicious computer program which is used to hack into a computer by misleading users of its true intent, it does not have the ability to replicate itself however, it can lead to viruses being installed on a machine since they allow the computer to be controlled by its creator.

trojan horse virus

It is a trial-and-error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort rather than employing intellectual strategies.

Brute force

Find the N value in the formula c=m^e mod N, if p = 389; q = 719

279691

Find the totient or φN.

p=283; q=101; **28200**

p=22; q=313; **6552**

p=917; q=179; **163048**

p=907; q=881; **797280**

p=241; q=887; **212640**

Using the steps in RSA algorithm, find the possible number for e or the encryption key. if p = 2; q = 13

11, **5**, **7**, **13**

Using the steps in RSA algorithm, find the possible number for e or the encryption key. if p = 2; q = 13; e = 11

11

Is a trusted entity that manages and issues security certificates and public keys that are used for secure communication in a public network. Its job is to issue certificates, to verify the holder of a digital certificate, and to ensure that holders of certificates are who they claim to be.

certificate authority

Find the co-primes of the result and given numbers, if p = 3 and q = 7

12

Find the co-primes of the result and given numbers, if p = 3 and q = 7 1. What are the co-primes?

10, 17, 20, 13, 19

Identify the following assurances that Digital signatures use by matching column A with Column B

The digital signature helps to assure that the signer is who he or she claims to be.	**Authenticity**
The digital signature helps to assure that the content has not been changed or tampered with since it was digitally signed.	**Integrity**
The digital signature helps prove the origin of the signed content to all parties. "Repudiation" refers to the act of a signer denying any association with the signed content.	**Nonrepudiation**
If an attacker edits the data, the digital signature verification at the receiver end fails. The hash of updated data and the verification algorithm's result will not match. As a result, the receiver can securely reject the message.	**Integrity**
When a verifier validates a digital signature using sender's public key, he is confident that the signature is of the sender with associated secret private key.	**Authenticity**
Because the signature key is known only to the signer, he can create a unique signature on a given data. In the event of a future disagreement, the receiver might offer the data and digital signature to a third party as evidence.	**Nonrepudiation**

Which of the following requirements must be met in order to digitally sign a form or form template? Choose all that apply.

The signing person or organization, known as the publisher, is trusted.

The digital signature is valid

The certificate associated with the digital signature is current (has not expired).

The certificate associated with the digital signature is issued to the publisher by a trusted certificate authority (CA).

Which of the following provides the security benefits of a digital certificate? Choose all that apply.

It contains the information that is required to identify and contact the issuing authority.

It contains personal information to help identify and trace the owner.

It is designed to be tamper-resistant and difficult to counterfeit.

It is issued by an authority that can revoke the identification card at any time (for example, if the card is misused or stolen).

It can be checked for revocation by contacting the issuing authority.

Identify the characteristic between a digital certificate and digital signature by matching Column A with Column B

digital signature – It verifies the identity of the document.

digital signature – It is issued to a specific individual by an authorized agency.

digital signature – It ensures that the signer cannot non-repudiate the signed document.

digital signature – It works on DSS (Digital Signature Standard)

digital certificate – It verifies the identity of the ownership of an online medium.

digital certificate – It is issued after the background check of the applicant by the Certificate Authority(CA).

digital certificate – It ensures that two parties who are exchanging the information are secured.

digital certificate – It works on the principles of public-key cryptography standards.

digital certificate – It contains personal information to help in identifying the trace of the owner.

This security feature and method used in digital signatures employ a long string of letters and numbers that represents the sum of the correct digits in a piece of digital data, against which comparisons can be made to detect errors or changes. It acts as a data fingerprint.

Checksum

This feature provides benefits by providing the data and time of a digital signature, timestamping is useful when timing is critical, such as for stock trades, lottery ticket issuance, and legal proceedings.

Timestamping

This is a technique that is used to protect data and messages from being tampered with. It is a one-way process that converts a message or data into a fixed-length code that cannot be reverse-engineered. This technique is used in various scenarios such as storing passwords, verifying file integrity, and generating digital signatures.

Hashing algorithm

It is a Federal Information Processing Standard(FIPS) that defines algorithms that are used to generate digital signatures with the help of the Secure Hash Algorithm(SHA) for the authentication of electronic documents.

Digital signature standard

This is a class of cryptographic protocols based on algorithms that require two separate keys, one that is private or secret, and one that is public.

Public key cryptography

It is an asymmetric system or algorithm that is used for public key cryptography, which is commonly used when sending secure, sensitive data over an insecure network like the internet.

rsa