Security+ SY0-601

Module 6
Cryptography.

aci LEARNING [HUBS]

Table of Contents.

1 Cryptographic Algorithms.

2 Cryptographic Uses.

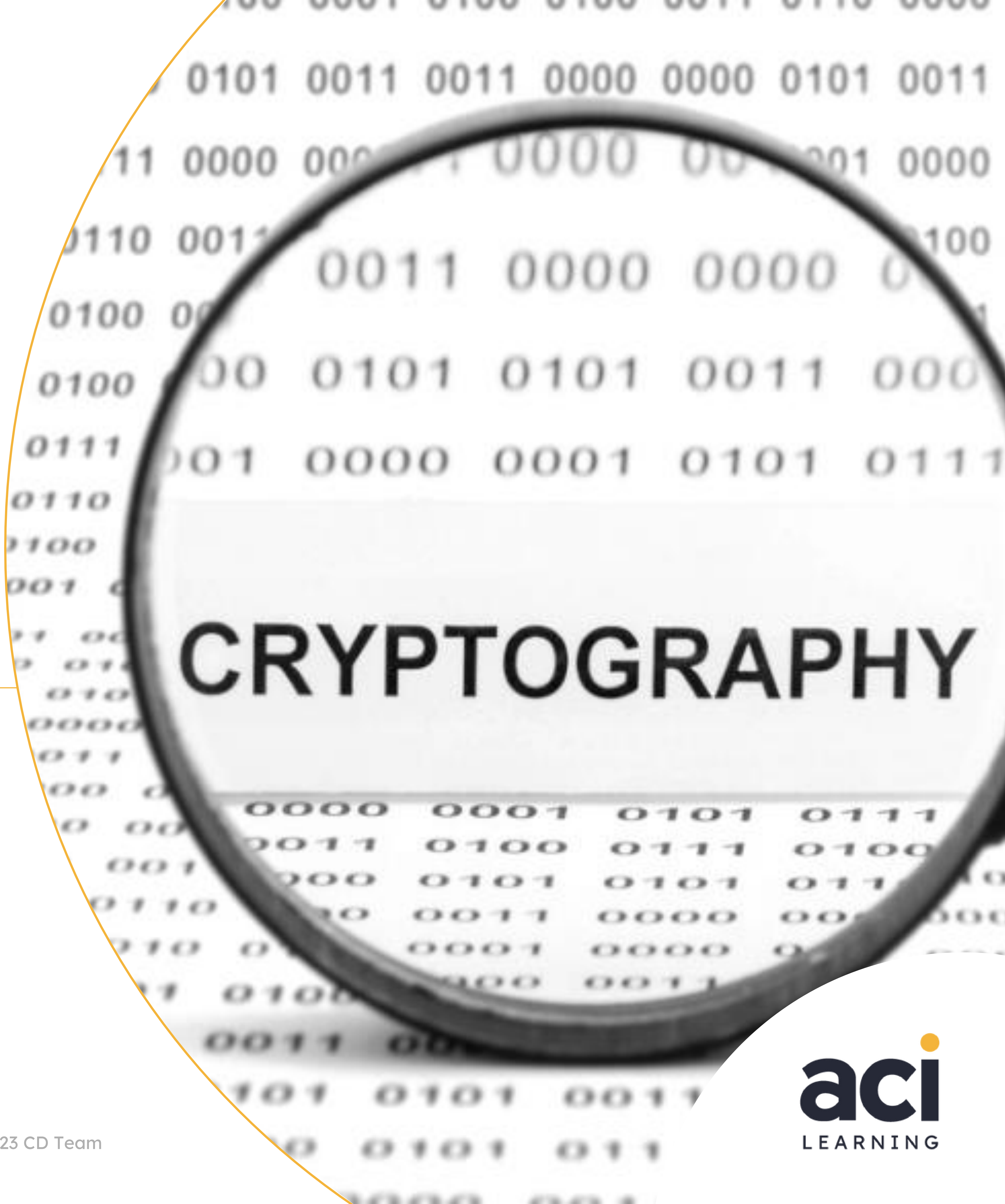
3 Public Key Infrastructure.

Learning objectives.

Upon completion of this module, you should be able to:

- Explain the purpose of cryptography and why different algorithms are used.
- Define the different uses for cryptography.
- Define what Public Key Infrastructure is and how it works.

Cryptographic Algorithms.



CRYPTOGRAPHIC ALGORITHMS.

Key concepts.

In this section, we will cover the following key concepts:

- Encryption Concepts.
- Ciphers.
- Algorithms.
- Keys.
- Symmetric.
- Asymmetric.
- Ephemeral Key.
- Elliptical Curve.
- Key Management.
- Cipher Suites.
- Hashes.
- Salting.

CRYPTOGRAPHIC ALGORITHMS.

Encryption concepts.

Encryption provides methods of enhancing confidentiality without hiding the data being transmitted. Rather, encryption serves the purpose of making data incomprehensible to bad actors.

Encryption types are based on their purpose. At the most basic level, encryption is converting plaintext (easily readable text) to ciphertext (plaintext scrambled through some sort of cipher or algorithm).

CONTINUED ON NEXT SLIDE >

CRYPTOGRAPHIC ALGORITHMS.

Encryption concepts.

Encryption typically involves a mixture of transposition and substitution. Transposition involves reordering the characters, while substitution involves replacing a character with a different character.

Transposition might look like “holeiwrdol,” in which the characters spelling out “Hello World” have been moved around. ROT13 is a basic example of substitution, in which the letter “a” is substituted with a letter 13 positions ahead: “uryyb jbryq” again translates to “hello world.”

CRYPTOGRAPHIC ALGORITHMS.

Ciphers.

Even though a basic algorithm is designed to be efficient, different cipher modes are implemented to make the algorithm efficient in concealing patterns.

- Electronic Code Book is the weakest mode.
- Errors in Cipher Block Chaining affect the whole chain.
- Cipher Feedback (CFB) works as a stream cipher.
- Output Feedback (OFB) works as a stream cipher.
- Counter Mode (CTR) is the strongest mode.
- Galois/Counter Mode (GCM) is a powerful mode.

CONTINUED ON NEXT SLIDE >

CRYPTOGRAPHIC ALGORITHMS.

Ciphers.

Stream ciphers encrypt the plaintext to ciphertext, either one bit or one byte at a time. These ciphers tend to be easier to reverse but are faster than block ciphers and are, therefore, useful in audio and video streaming. RC4 is an example of a stream cipher used with WEP and WPA for wireless encryption.

Stream ciphers are symmetric key algorithms.

It is important to understand that stream ciphers are typically faster but less secure than block ciphers.

CONTINUED ON NEXT SLIDE >

CRYPTOGRAPHIC ALGORITHMS.

Ciphers.

Block ciphers encrypt the plaintext to the ciphertext in blocks of bits, most commonly 64-bit blocks; these ciphers tend to be harder to reverse but are also slower to use than stream ciphers.

DES, Triple DES, and AES are well-known block ciphers, though DES is no longer considered secure.

These three are also well-known symmetric key algorithms.

CRYPTOGRAPHIC ALGORITHMS.

Algorithms.

Per the Merriam-Webster online dictionary, an algorithm is a procedure for solving a mathematical problem (as in finding the greatest common divisor) in a finite number of steps that frequently involve the repetition of an operation.

More broadly, an algorithm is a step-by-step procedure for solving a problem or accomplishing some end.

Algorithms can be used for many purposes, but for this discussion, most will be of a mathematical nature and are generally related to calculating some complex value like a ciphertext block.

CRYPTOGRAPHIC ALGORITHMS.

Keys.

Keys are used with algorithms to encrypt and decrypt data, packets, and other bits of information that need to be kept confidential. Keys may be generated through algorithms, generally requiring entropy or randomly-generated values for input.

Keys may be symmetric or asymmetric; both are useful but have their own advantages and disadvantages.

The longer the key length (of the same encryption standard), the harder it is to break; however, lengthier keys are more resource-intensive in contrast to short keys.

- 128 vs. 256
- 256 vs. 512
- 1024 vs. 2048
- 2048 vs. 4096

CRYPTOGRAPHIC ALGORITHMS.

Symmetric key encryption.

Symmetric encryption uses the same key to decrypt data that was used to encrypt it.
The current standard for symmetric key length is 256 bits.

All session keys are symmetric keys, but not all symmetric keys are session keys.

Symmetric keys are generated for a single session, such as one to login to your bank.
Session keys are used for one session, with other session keys generated for subsequent sessions.

Symmetric keys have a couple of issues.

First, symmetric algorithms involve many keys for multiple people to communicate securely.

Second, you need a way to securely share the key with whomever communications are being exchanged.

CONTINUED ON NEXT SLIDE >

CRYPTOGRAPHIC ALGORITHMS.

Symmetric key concerns.

Symmetric keys are generated by one party to a conversation but must be securely delivered to any other party. You can't use the same connection you want to encrypt, as anyone listening will receive the keys too.

Emailing the keys or texting is impractical due to the length of the keys (lots of opportunities to type something incorrectly) and, frankly, also takes too long if you want to communicate now.

Additionally, symmetric key encryption can involve a lot of keys — for 100 users to each have separate, secure communications with each of the other 99 users would require a LOT of keys.

CRYPTOGRAPHIC ALGORITHMS.

Symmetric key encryption.

Here's the math:

$N(N - 1)/2$ where N equals the number of users.

100(100-1)/2

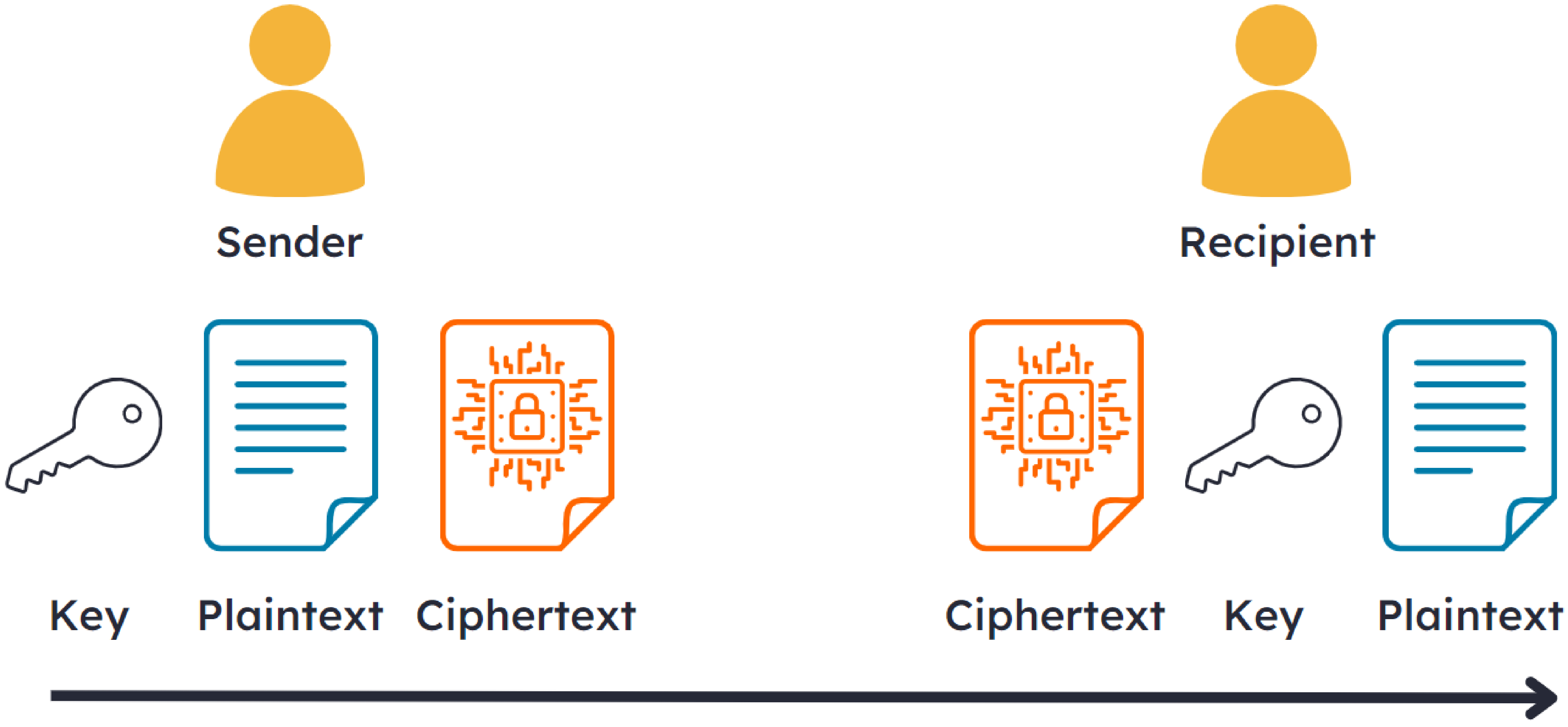
100(99)=9900

9900/2=4950

For 100 users to communicate securely with each of the other 99 users would require 4,950 keys – and they have to be delivered securely on top of that!

CRYPTOGRAPHIC ALGORITHMS.

Symmetric key encryption.



CRYPTOGRAPHIC ALGORITHMS.

Symmetric encryption.

- Advanced Encryption Standard (AES) is the current standard in symmetric encryption; it is used in WPA2 and WPA3 as well as in many cryptographic suites. The minimum key length recommended today is a 256-bit key.

- Data Encryption Standard (DES), once the standard used by the Government and the Military, DES has aged. Triple DES (3DES) uses three 56-bit keys (effectively a 168-bit key) and modes like 3EEE and 3EDE.

CONTINUED ON NEXT SLIDE >

CRYPTOGRAPHIC ALGORITHMS.

Symmetric encryption.

- Blowfish serves a similar purpose to the others and is used in cipher suites interchangeably, but like DES, it has aged. Blowfish's creator, Bruce Schneier, recommends Twofish for modern applications.
- Rivest Cipher 4 (RC4) is a stream cipher — the only pure stream cipher on this list. RC4 is fast but not strong and is the algorithm used in WEP and the default used in WPA.

CRYPTOGRAPHIC ALGORITHMS.

Asymmetric.

Asymmetric encryption uses one key for encryption and a different key for decryption. Asymmetric keys tend to be much stronger and are often held and used for a longer period.

Asymmetric key encryption takes many forms but is perhaps most commonly implemented as part of Public Key Infrastructure (PKI), involving a digital certificate with an associated public key and private key.

The public key is freely available to anyone and can be sent without the need for a secure means, as it is only used to encrypt content to the holder of the private key. The private key is closely held and must be kept secret, as it is used to decrypt encrypted communications.

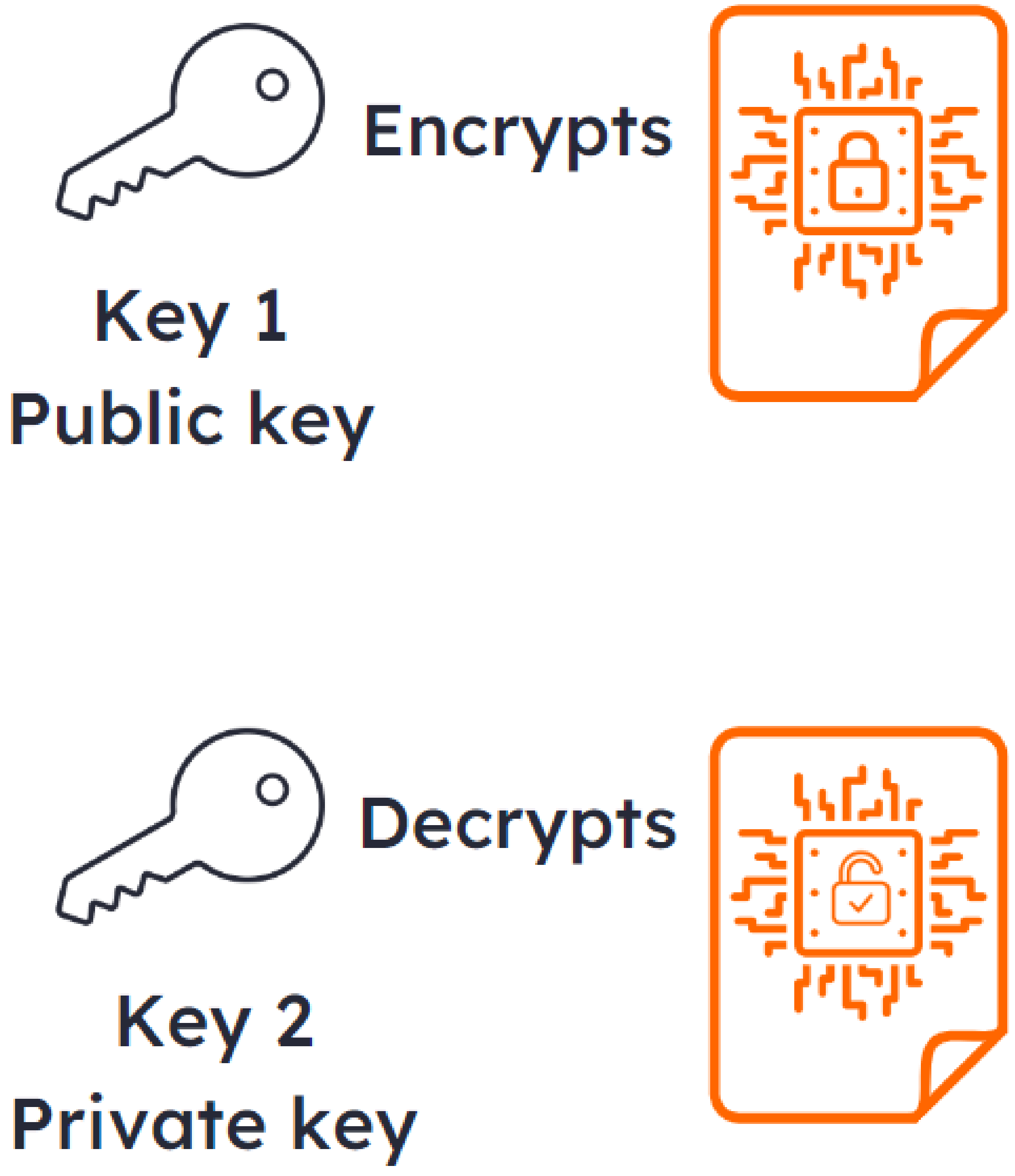
CONTINUED ON NEXT SLIDE >

CRYPTOGRAPHIC ALGORITHMS.

Asymmetric.

The digital certificate can be used to authenticate the sender and provides for encrypted communications, among other uses.

Only the private key can decrypt something encrypted with the public key AND only the public key can decrypt something encrypted with the private key.

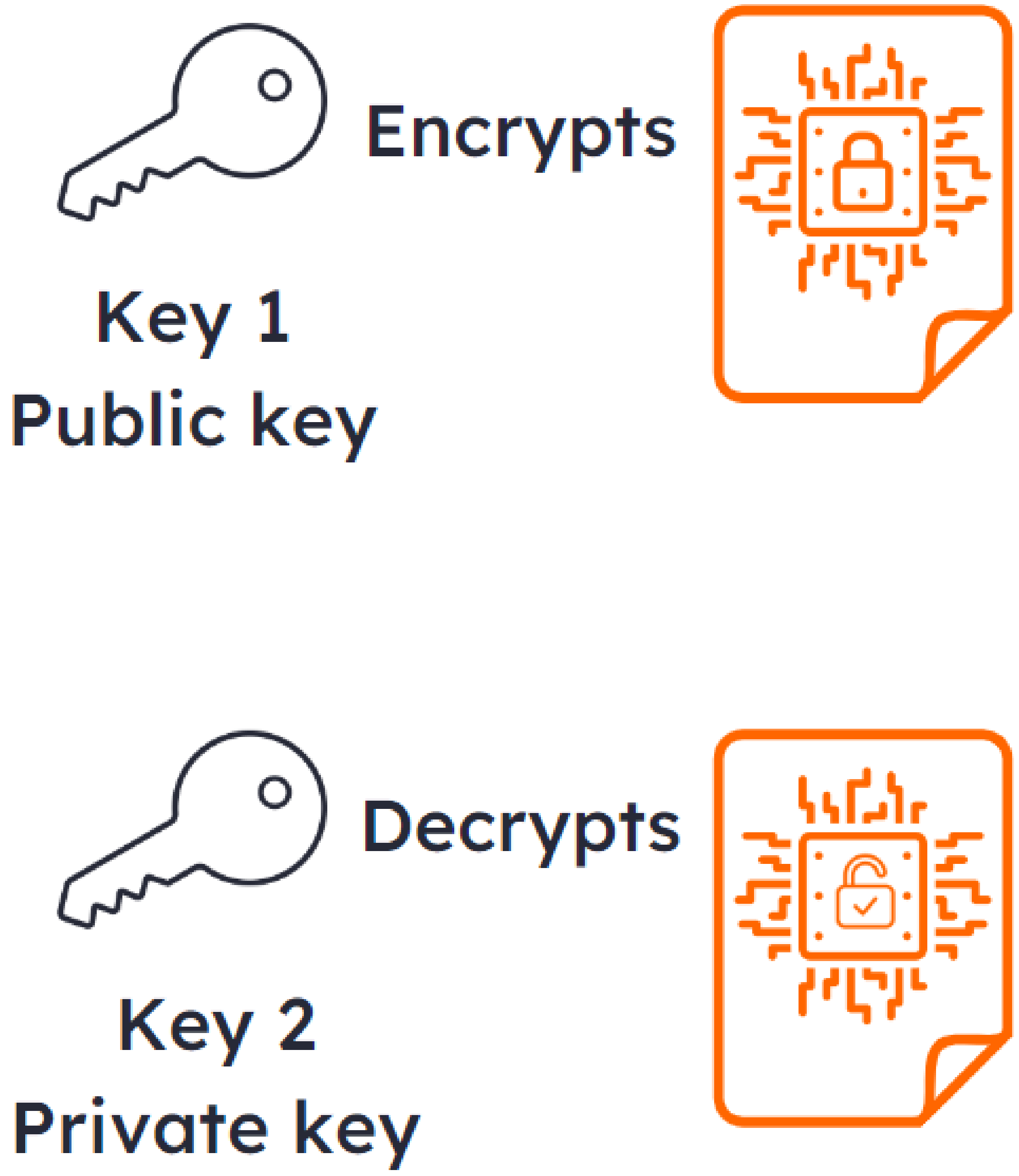


CRYPTOGRAPHIC ALGORITHMS.

Asymmetric key concerns.

Asymmetric encryption uses longer, stronger keys, which makes for safer communications, and allows a key to be employed for a longer time, but it also means that encryption takes longer and is more resource intensive. The size of the data that can be encrypted is limited by the size of the asymmetric key length. This means that asymmetric encryption is not good for encrypting large amounts of data.

The current standard for asymmetric key length is 2048 bits; this makes it hard to crack encryptions that use such keys. Asymmetric encryption also uses fewer keys for larger numbers of people — for 100 people to securely encrypt content to each of the others in a way that the other 98 couldn’t read would require 100 private key/public key pairs or a mere 200 keys; however, if everyone used asymmetric encryption for the bulk of their communications, the processing delays would get out of control on sites with lots of traffic.



Encrypts

Key 1

Public key

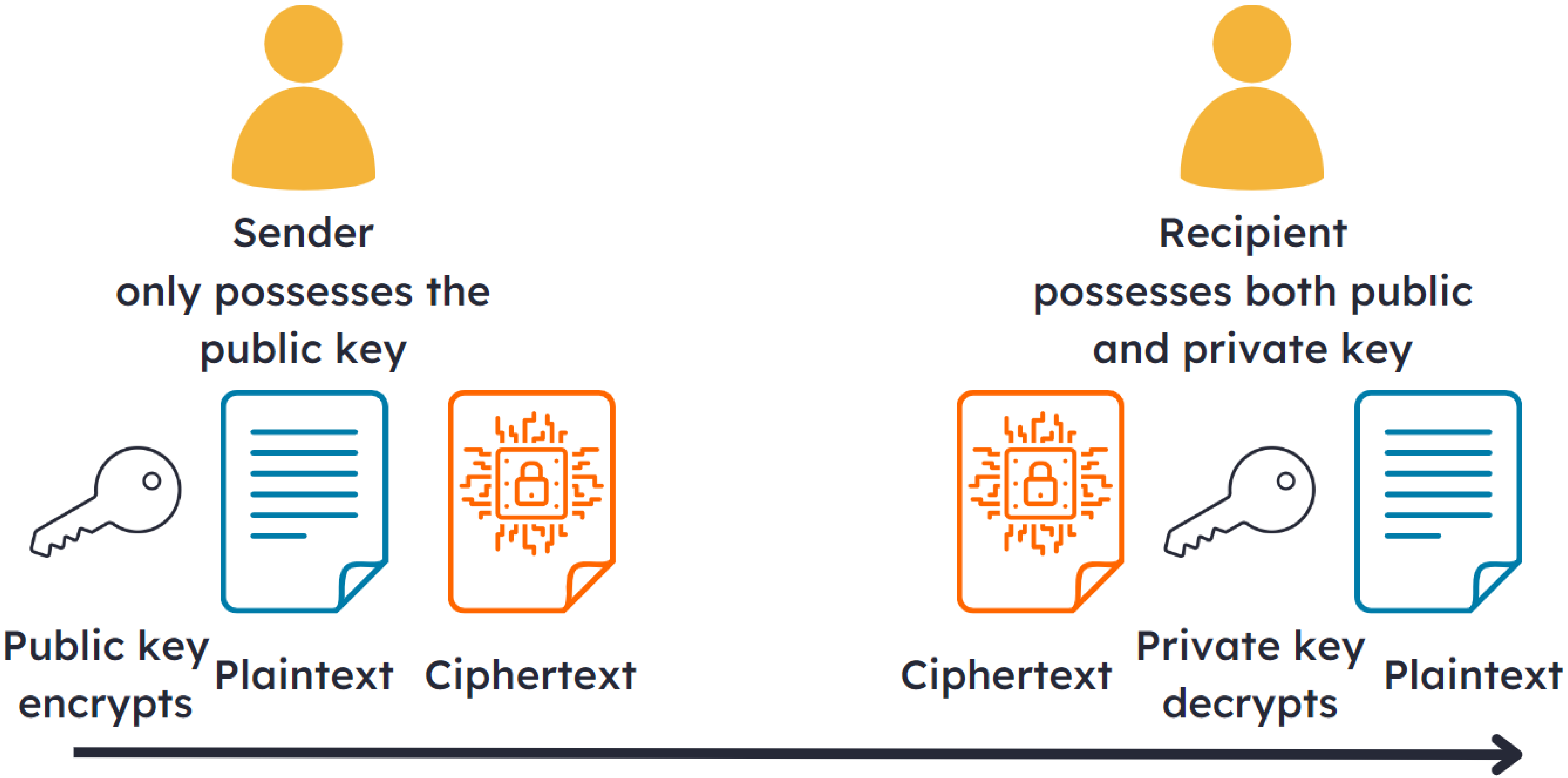
Decrypts

Key 2

Private key

CRYPTOGRAPHIC ALGORITHMS.

Asymmetric.



Sender
only possesses the
public key

Recipient
possesses both public
and private key

CRYPTOGRAPHIC ALGORITHMS.

Asymmetric encryption.

- Rivest, Shamir, and Adelman (RSA) are one of the oldest key exchange algorithms; it is still commonly used today in digital certificates, typically with a 2048-bit key. Its keys are two very large prime numbers.

- Diffie-Hellman (DH) is another widely-used key exchange algorithm; as with RSA, a 2048-bit key is recommended. DH uses asymmetric encryption for two parties to create the same symmetric key independently.

CONTINUED ON NEXT SLIDE >

CRYPTOGRAPHIC ALGORITHMS.

Asymmetric encryption.

- Digital Signature Algorithm (DSA) is an algorithm commonly used for digital signatures, which provides both authentications of the signer and integrity of the document.
- ElGamal is based on the Diffie-Hellman Key Exchange, and like the DH and RSA, it is a public key cryptographic algorithm. DSA is also based on ElGamal’s signature scheme.

CRYPTOGRAPHIC ALGORITHMS.

Ephemeral keys.

Ephemeral keys are asymmetric encryption keys that are generated for each key exchange; they may be used more than once in a single session.

Ephemeral keys are generated and used for a very short period only; the short period for ephemeral key use is designed to prevent a key from being compromised and used in related attacks or replay attacks. This provides protection for previous and future sessions if an ephemeral key is compromised. This is called Perfect Forward Secrecy.

CRYPTOGRAPHIC ALGORITHMS.

Elliptical curve (EC).

- Elliptical curve (EC), also known as elliptical curve cryptography, is an asymmetric encryption algorithm that leverages the algebraic structures of elliptic curves over finite fields to derive public/private key pairs.
- The elliptical curves being graphed can span miles, producing a large number of points from which the keys are generated.
- EC is a type of trapdoor function that is easy to perform using the public key but difficult to reverse without knowing the private key.

CRYPTOGRAPHIC ALGORITHMS.

Key management.

Key management is the act of managing cryptographic keys. Core key management activities include:

- Generation
- Exchange
- Usage
- Storage
- Renewal
- Archival
- Recovery
- Destruction

CRYPTOGRAPHIC ALGORITHMS.

Cipher suites.

- Cipher suites were generated to identify specific types of encryption on information based on four basic elements:
  - The key exchange algorithm.
  - The authentication algorithm.
  - The bulk encryption algorithm.
  - The Message Authentication Code (MAC) algorithm.
- A given computer will likely support a variety of cipher suites, allowing it to negotiate which suite to employ in communications with other systems.

CRYPTOGRAPHIC ALGORITHMS.

Cipher suites.

As noted, cipher suites typically have four elements. As noted on JSCAPE.com, these are as follows:

- The Key Exchange Algorithm — This is the asymmetric algorithm used to exchange the symmetric key used for bulk encryption. Common examples include RSA, DH, ECDH, & ECDHE.
- The Authentication Algorithm — This component dictates how server authentication and possibly client authentication (if required) will be conducted. Examples are RSA, DSA, and ECDSA.

CONTINUED ON NEXT SLIDE >

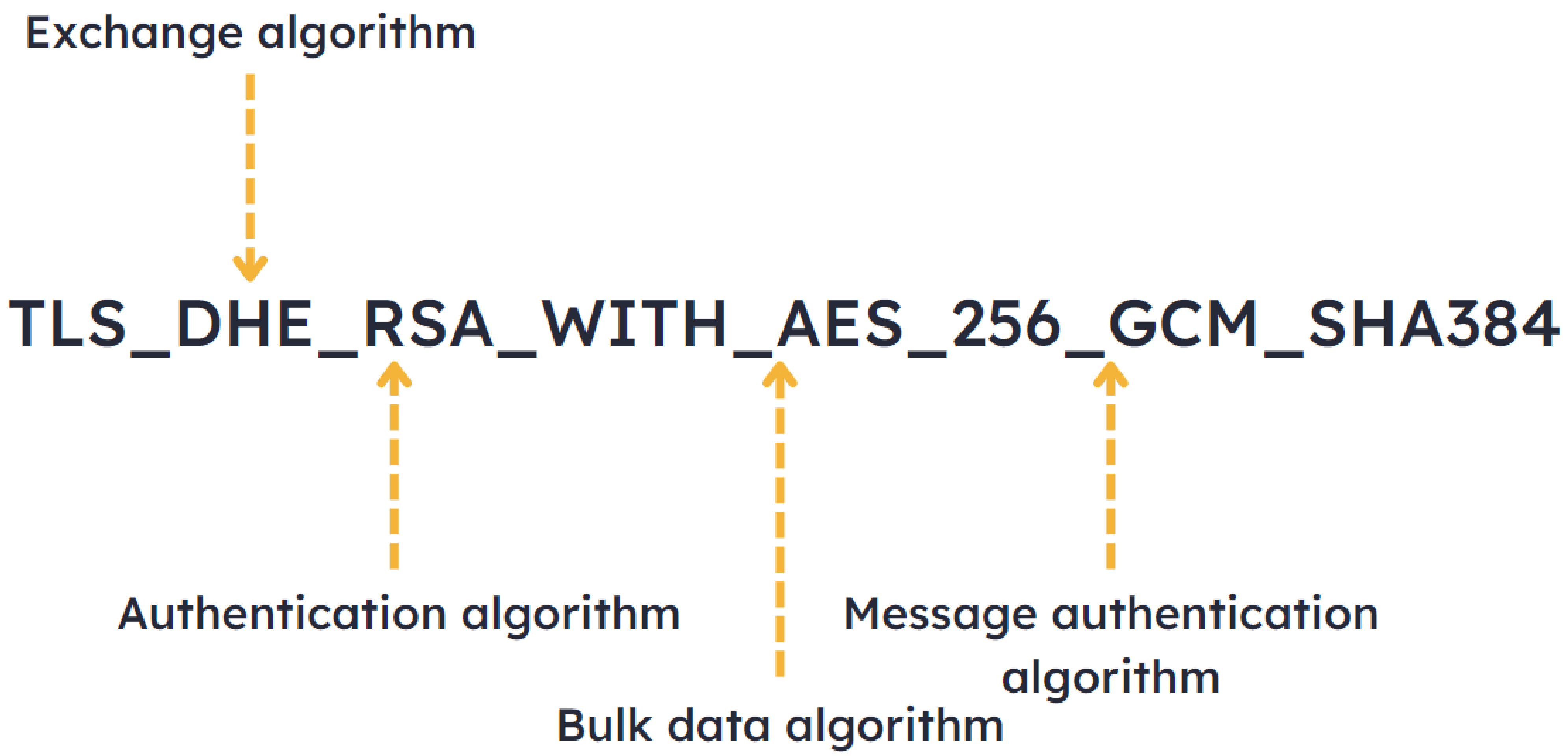
CRYPTOGRAPHIC ALGORITHMS.

Cipher suites.

- The Bulk Encryption Algorithm — This is the symmetric key algorithm used to encrypt most of the session transmissions; examples include AES and 3DES.
- The Message Authentication Code (MAC) Algorithm — The function of this component is to verify the integrity of any messages exchanged. SHA and MD5 serve in this role commonly.

CRYPTOGRAPHIC ALGORITHMS.

Cipher suites.



Exchange algorithm

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

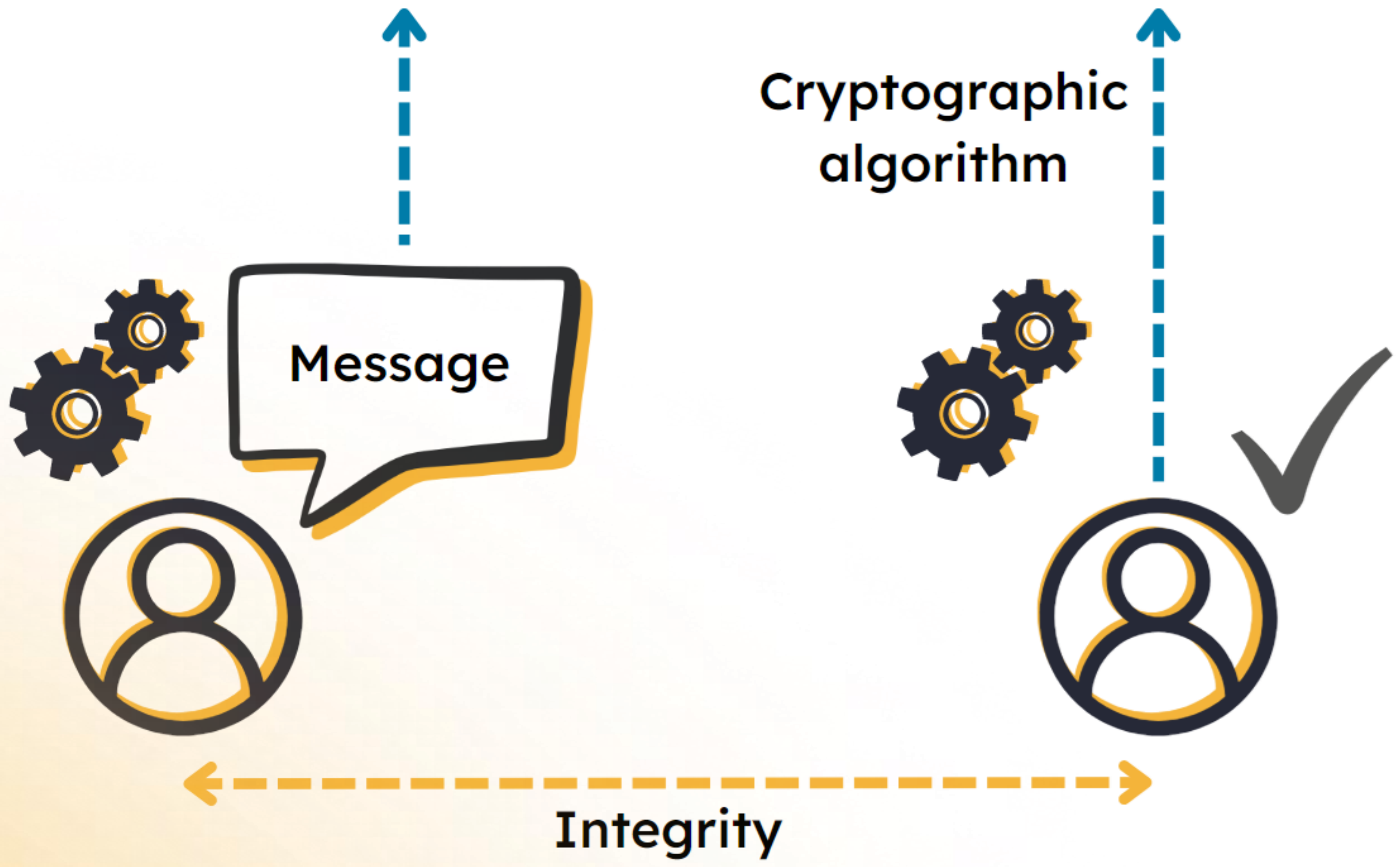
Authentication algorithm

Bulk data algorithm

Message authentication algorithm

CRYPTOGRAPHIC ALGORITHMS.

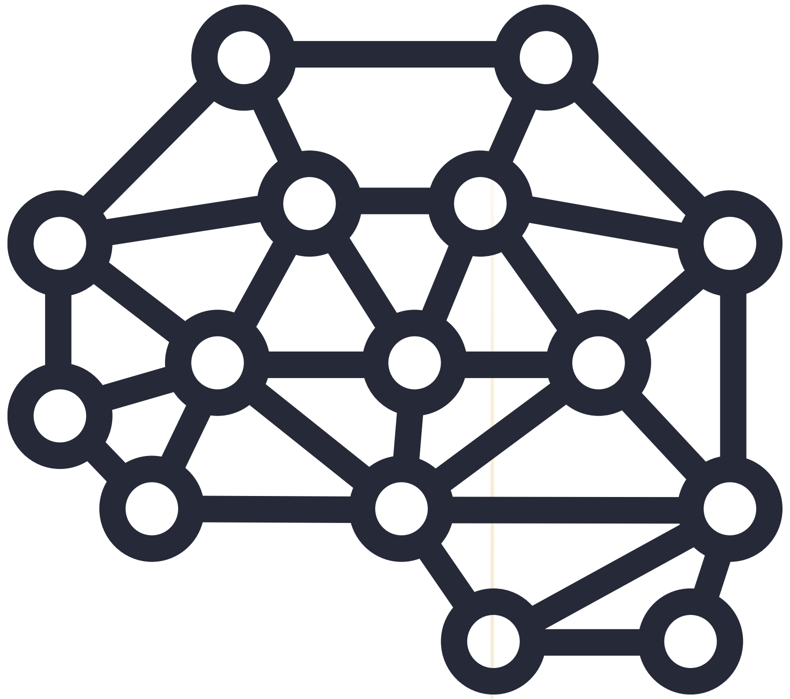
Cipher suites.



- Hashes are one-way (not reversible) cryptographic algorithms that generate an alphanumeric output based on the contents of a file, communication, or password, for instance.
- Hashes can be used to prove the integrity of a file or that a correct password has been entered. Hashes are also used to check that a software installation file has not been altered.
  MD5 (Message Digest 5) and SHA (Secure Hashing Algorithm) are two well-known hashes.

CRYPTOGRAPHIC ALGORITHMS.

Hashing algorithms.



Message Digest 5 (MD5)

- 128-bit
- Weakest
- Prone to collisions

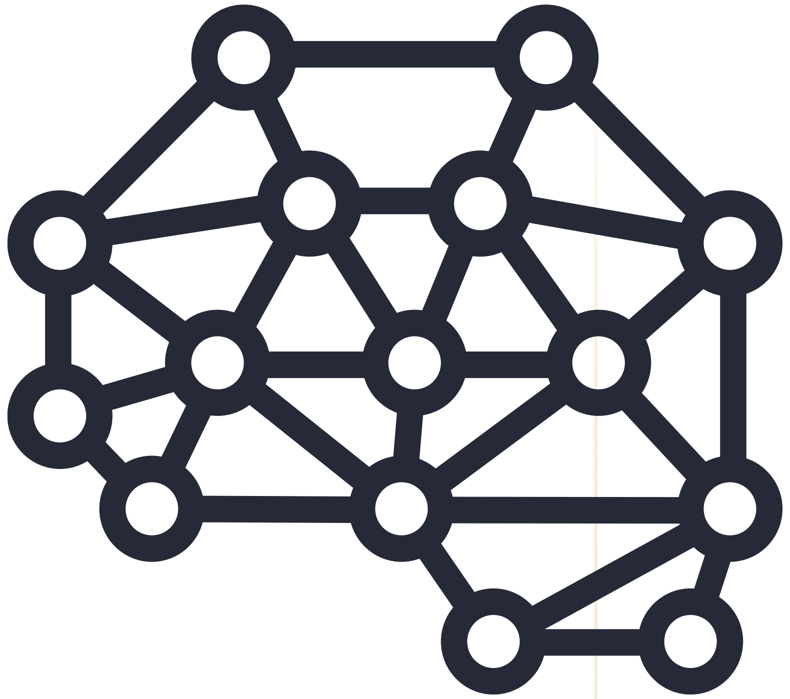
Secure Hashing Algorithm - 1 (SHA-1)

- Successor to MD5
- 160-bit
- Collision attacks

CONTINUED ON NEXT SLIDE >

CRYPTOGRAPHIC ALGORITHMS.

Hashing algorithms.



Secure Hashing Algorithm - 2 (SHA-2)

- Successor to SHA-1
- 224, 256, 384, and 513-bits
- Strongest

RIPEMD

- Designed as a replacement for MD5
- 128, 160, 256, and 320-bit variants

CRYPTOGRAPHIC ALGORITHMS.

Hashing algorithms.

Cyclic Redundancy Check (CRC) Considerations:

- Used for message integrity verification.
- 16, 32, and 54-bit variants.

Hashed Message Authenticate Code (HMAC) Considerations:

- Data integrity and authenticity.
- Keyed hashing function.
- Used with MD5, SHA-1, and SHA-2.

CRYPTOGRAPHIC ALGORITHMS.

Salting.

Salt is the addition of random values to a password or key before hashing it. Salting alters and lengthens the original value so that attempts to brute force are more difficult. The hash represents both a longer password value, which will significantly lengthen the time required to crack it, and a different value than the actual password.

CRYPTOGRAPHIC ALGORITHMS.

Knowledge check.

Let's apply what we have covered:

- Describe the differences between symmetric and asymmetric encryption.
- What is the main function of hashing?

Cryptographic Uses.

CRYPTOGRAPHIC USES.

Key concepts.

In this section, we will cover the following key concepts:

- Key exchange.
- Key Stretching.
- Data in Transit.
- Digital Signatures.
- Message Authorization Code.

CONTINUED ON NEXT SLIDE >

CRYPTOGRAPHIC USES.

Key concepts.

In this section, we will also cover the following key concepts:

- Data at Rest.
- Full Disc Encryption.
- Encrypting File System.
- Steganography.
- Security Accounts Manager.

CONTINUED ON NEXT SLIDE >

CRYPTOGRAPHIC USES.

Key concepts.

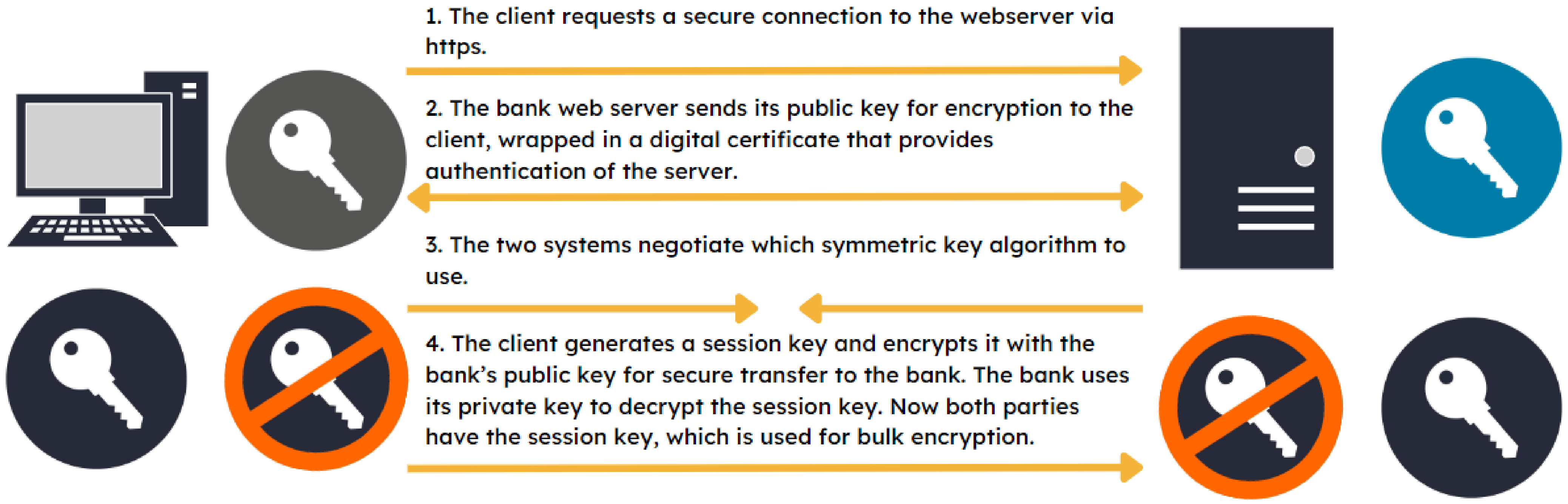
In this section, we will also cover the following key concepts:

- Checksums.
- VPNs.
- IPSec.
- PFS.
- Homomorphic Encryption.

CRYPTOGRAPHIC USES.

Key exchange.

Key exchange can be facilitated by using asymmetric encryption to securely exchange a (symmetric) session key, which then alleviates the delays associated with asymmetric encryption by using the session key for bulk encryption. Imagine you are connecting to your bank's website:



1. The client requests a secure connection to the webserver via https.

2. The bank web server sends its public key for encryption to the client, wrapped in a digital certificate that provides authentication of the server.

3. The two systems negotiate which symmetric key algorithm to use.

4. The client generates a session key and encrypts it with the bank's public key for secure transfer to the bank. The bank uses its private key to decrypt the session key. Now both parties have the session key, which is used for bulk encryption.

CRYPTOGRAPHIC USES.

Key stretching.

Key stretching is a way to strengthen weak passwords by generating a derived key through various repetitive steps, such as salting and hashing a password and repeating this process to produce a longer output each time; this process may involve thousands of iterations.

Two common key stretching algorithms are:

- BCRYPT: A password-hashing algorithm that uses a Blowfish cipher (symmetric block).
- PBKDF2: Password-Based Key Derivation Function 2 uses HMAC-SHA-1 by default.

CRYPTOGRAPHIC USES.

Digital signatures.

Digital signatures are a feature of Public Key Infrastructure. A digital signature is used to provide authentication and nonrepudiation. A hash is made of some content being exchanged, and the hash is encrypted with the private key of the sender. This is called the message digest. The hashed content is not meant to be confidential data.

The public key is used to decrypt the hash, which is compared to a hash of the original content conducted by the recipient using the same hashing algorithm as the sender. If the two hashes match, this serves as proof that the message digest was encrypted with the private key. Since the sender is the only one with that private key, the content must have been sent by that individual, ensuring nonrepudiation.

CRYPTOGRAPHIC USES.

Message authentication codes (MAC).

Message authentication codes (MAC) function in a similar way to digital signatures, providing authentication of the sender and proof of the document's integrity.

CRYPTOGRAPHIC USES.

Data in transit.

Data in transit is data that is being sent across network connections from one location to another. Sending and receiving encrypted web traffic between yourself and a server is an example of data in transit.

Data in transit is encrypted to prevent unauthorized viewing. HTTPS, SSL/TLS, and FTPS (FTP over SSL) are examples of protocols used to protect data in transit.

CRYPTOGRAPHIC USES.

Data at rest.

Data at rest refers to data that is in the storage on a hard disk or another storage device and not presently in use, nor in transit, that is, on its way to being used.

Data at rest is typically protected by encryption tools such as BitLocker or Encrypting File System (EFS) and with features like file permission and access control lists.

A trusted platform module (TPM, a cryptographic chipset on the motherboard) is often used to generate and store encryption keys for data at rest.

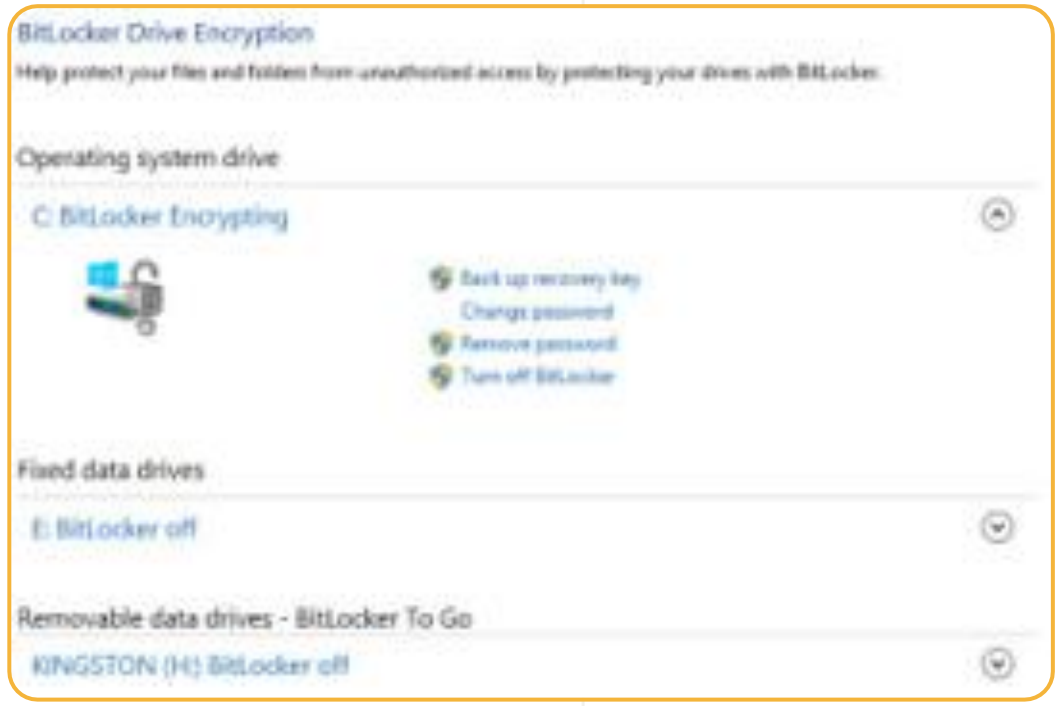
CRYPTOGRAPHIC USES.

Full disc encryption.

Full disc encryption (FDE) protects all files located on a drive against unauthorized access by encrypting the entire drive, as the name implies.

BitLocker is a Microsoft proprietary OS feature that will encrypt an entire storage drive.
BitLocker is available on professional, educational, and enterprise versions of Windows and works on both internal and removable storage.
BitLocker generally relies on the TPM, the trusted platform module, for key generation and storage, though other devices, such as a hardware security module, can also serve.

Drives encrypted with BitLocker will display a lock icon next to the drive letter to indicate this status.



BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker

Operating system drive

C: BitLocker Encrypting

Fixed data drives

E: BitLocker off

Removable data drives - BitLocker To Go

KINGSTON (H:) BitLocker off

CRYPTOGRAPHIC USES.

Encrypting file system (EFS).

Encrypting file system (EFS) is a component of the NTFS file system. It's available in Windows operating systems (professional, educational, and enterprise versions only) and uses a symmetric key in combination with public-key technology to encrypt individual files and directories.

Whereas BitLocker encrypts an entire drive, EFS encrypts a single file or directory. Files and folders that have been encrypted will display their names in green letters instead of the typical black file names used in Windows.

EFS is an example of file-level encryption (FLE).

CRYPTOGRAPHIC USES.

Stenography.

Steganography is the process of hiding content within other content using applications like QuickStego. Text, photos, and other content can be embedded in larger files, with or without actual encryption. The same software can extract the content that was originally embedded in it.

In essence, this allows content to be transmitted with its very presence concealed so that only the innocuous carrier file is visible to the naked eye.

CRYPTOGRAPHIC USES.

Security Accounts Manager (SAM).

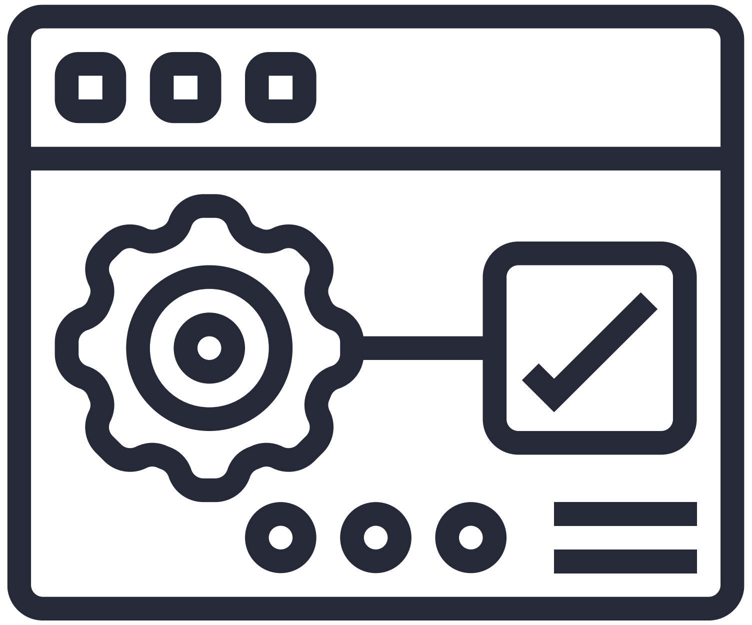
Security Accounts Manager (SAM) holds local login credentials stored as hashes of a password; as a user enters the password, the system hashes the entry and compares it to the stored hash.

CRYPTOGRAPHIC USES.

Checksums.

Checksums are mathematical summations of the data they are meant to check, similar to a hash and typically used to check the integrity of files or packets. Files in storage may be hashed when stored and checked later to determine whether they have been altered.

A checksum can't prevent modification; it can only detect that it has occurred. Checksums are often used on packet headers to detect altered packets, whether deliberate or due to a collision.



CRYPTOGRAPHIC USES.

Virtual private networks (VPNs).

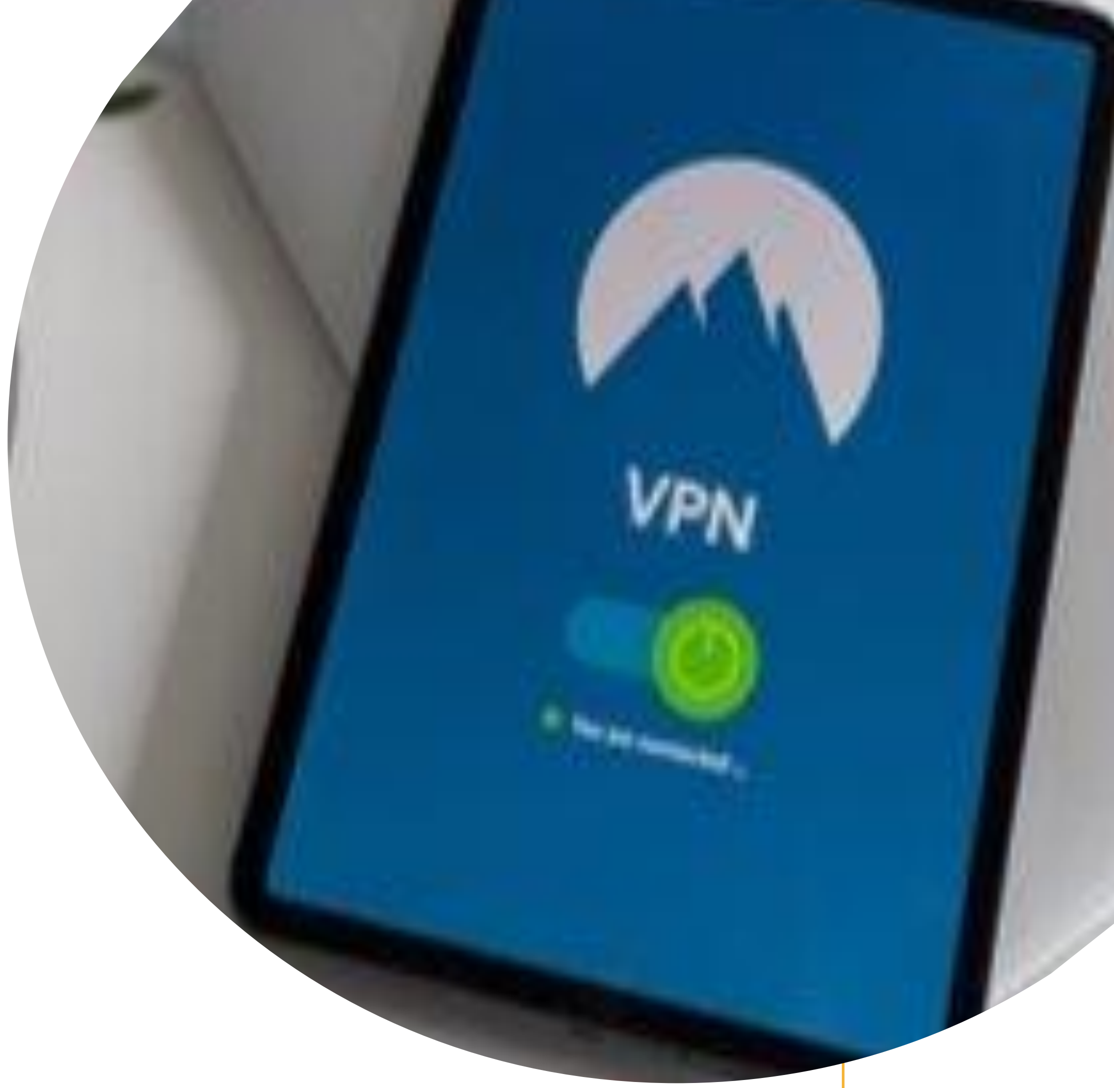
Virtual private networks (VPNs) are encrypted tunnels through which data travels securely through a public network like the Internet.

VPNs can be internal or external and may be host-to-host, site-to-host, or site-to-site.

The term tunnel here refers to the fact that the packets are encapsulated in outer packets.

CRYPTOGRAPHIC USES.

Virtual private networks (VPNs).



A tunnel is a private, secure connection between a network and an outside resource, such as another LAN or a VPN service provider. VPNs are heavily used when an organization requires secure, remote connections to a LAN. When an employee uses a VPN to connect to an office, that remote connection is protected with an encrypted tunnel. This connection is considered more trusted than a simple RDP or other basic remote connection.

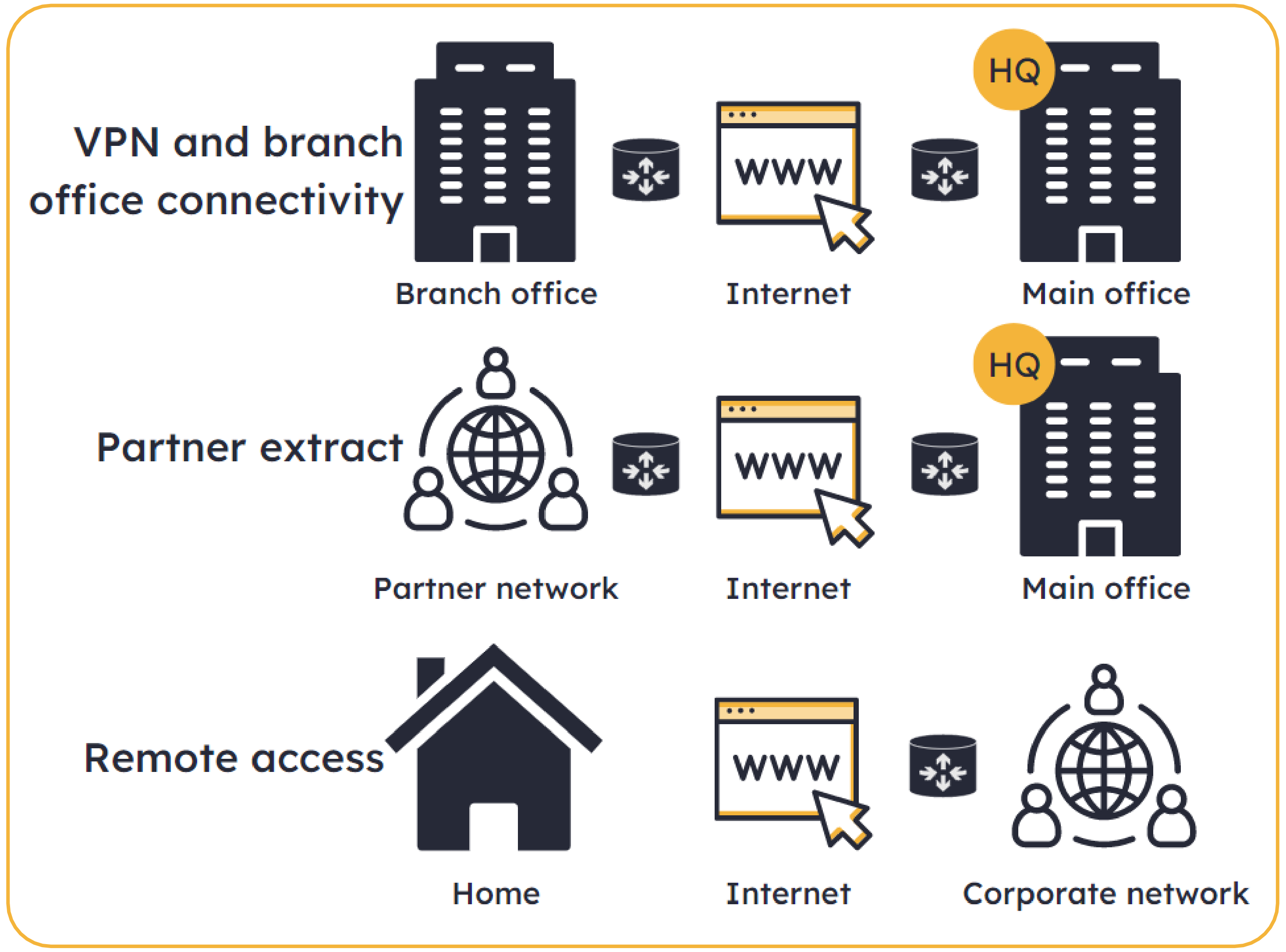
CRYPTOGRAPHIC USES.

IPSec.

IPSec is a protocol for encrypting a packet as part of a VPN deployment. While there are IPSEC VPNs, IPSEC is commonly used to secure L2TP tunnels.

Among the protocols that make up, IPSec is Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE), Internet Security Association, Key Management Protocol (ISAKMP), and Oakley.

IPSec also has a mode that can be set up in transport mode (encrypts the body only) or in tunnel mode (encrypts the body and the headers, adding IPSEC headers for delivery).



CRYPTOGRAPHIC USES.

IPSec.

PHASE 1 SA

- IKE Phase 1
- Main Mode
- Traffic Management

COMPONENTS

- Negotiation
- Authentication (PSK, Digital Certificate)
- DH Key Exchange
- Session Duration
- Encryption (DES, 3DES, AES)

PHASE 2 SA

- IKE Phase 1
- Quick Mode
- Data Exchange

COMPONENTS

- Negotiation
- IPSec Protocol (AH, ESP)
- Encapsulation (Transport vs. Tunnel)
- Authentication (MD5, SHA)
- Session Duration
- Optional DH Key Exchange (PFS)

CRYPTOGRAPHIC USES.

IPSec Protocols.

AUTHENTICATION HEADER (AH)

- Authentication
- Integrity
- IP Protocol 51
- Payload is not encrypted

ENCAPSULATING SECURE PAYLOAD (ESP)

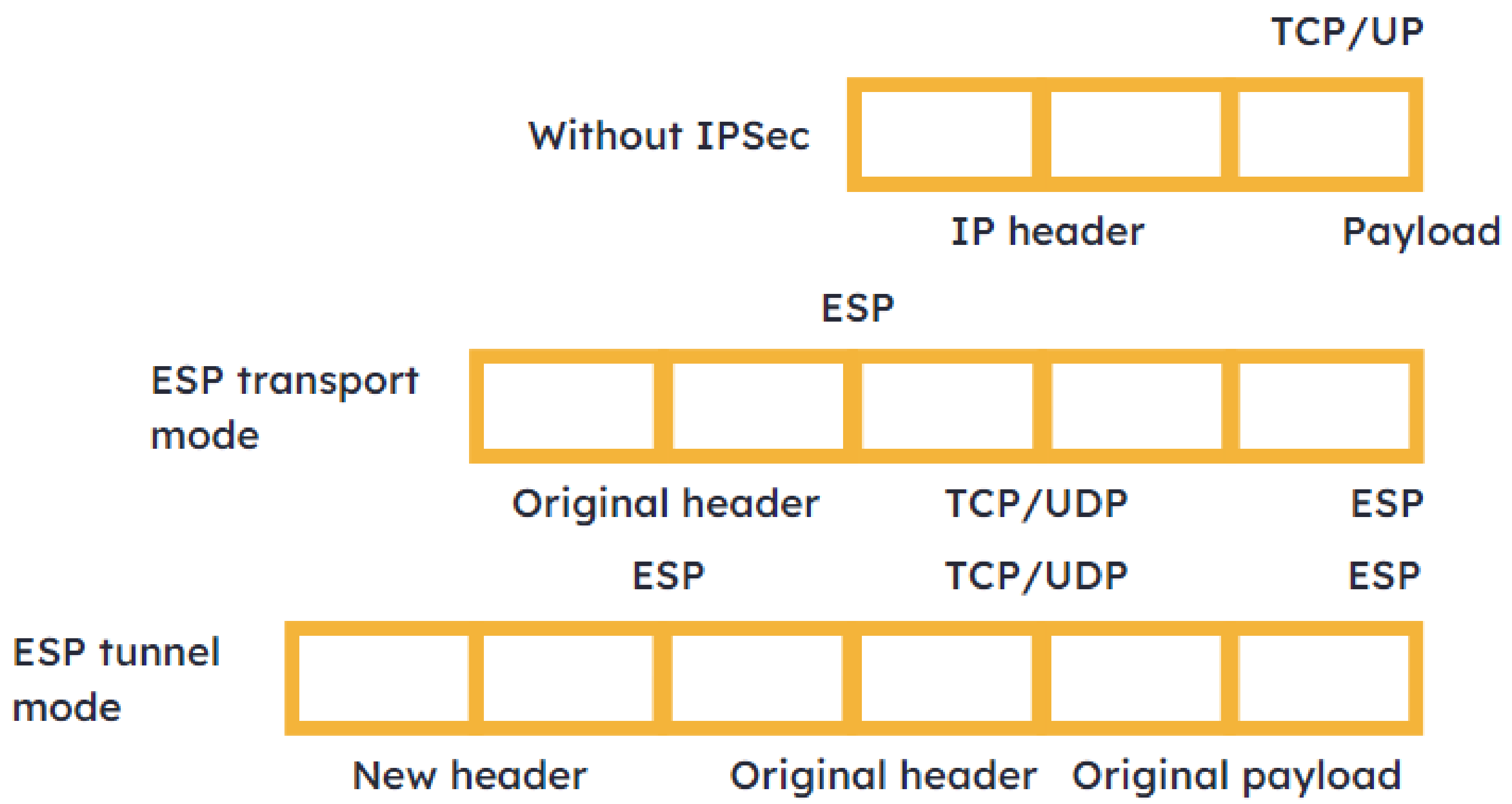
- Authentication
- Integrity
- Encryption/Confidentiality
- IP Protocol 50
- Payload and header are encrypted

CRYPTOGRAPHIC USES.

Transport and tunnel modes.

Transport mode is commonly used between a client and a server, workstation, and gateway.

Tunnel mode is the default, commonly used in gateway-to-gateway (router-to-router or site-to-site) across an unsecure network; it encrypts an entire packet and payload while adding a new header.



CRYPTOGRAPHIC USES.

Perfect forward secrecy.

Perfect forward secrecy (PFS) is created by the use of specific encryption protocols that generate keys in such a way that obtaining one of the (ephemeral session) keys will not help in cracking any of the others.

Two protocols are noted for providing PFS among all those we study: Diffie-Hellman Ephemeral (DHE) and Elliptical Curve Diffie-Hellman Ephemeral (ECDHE).

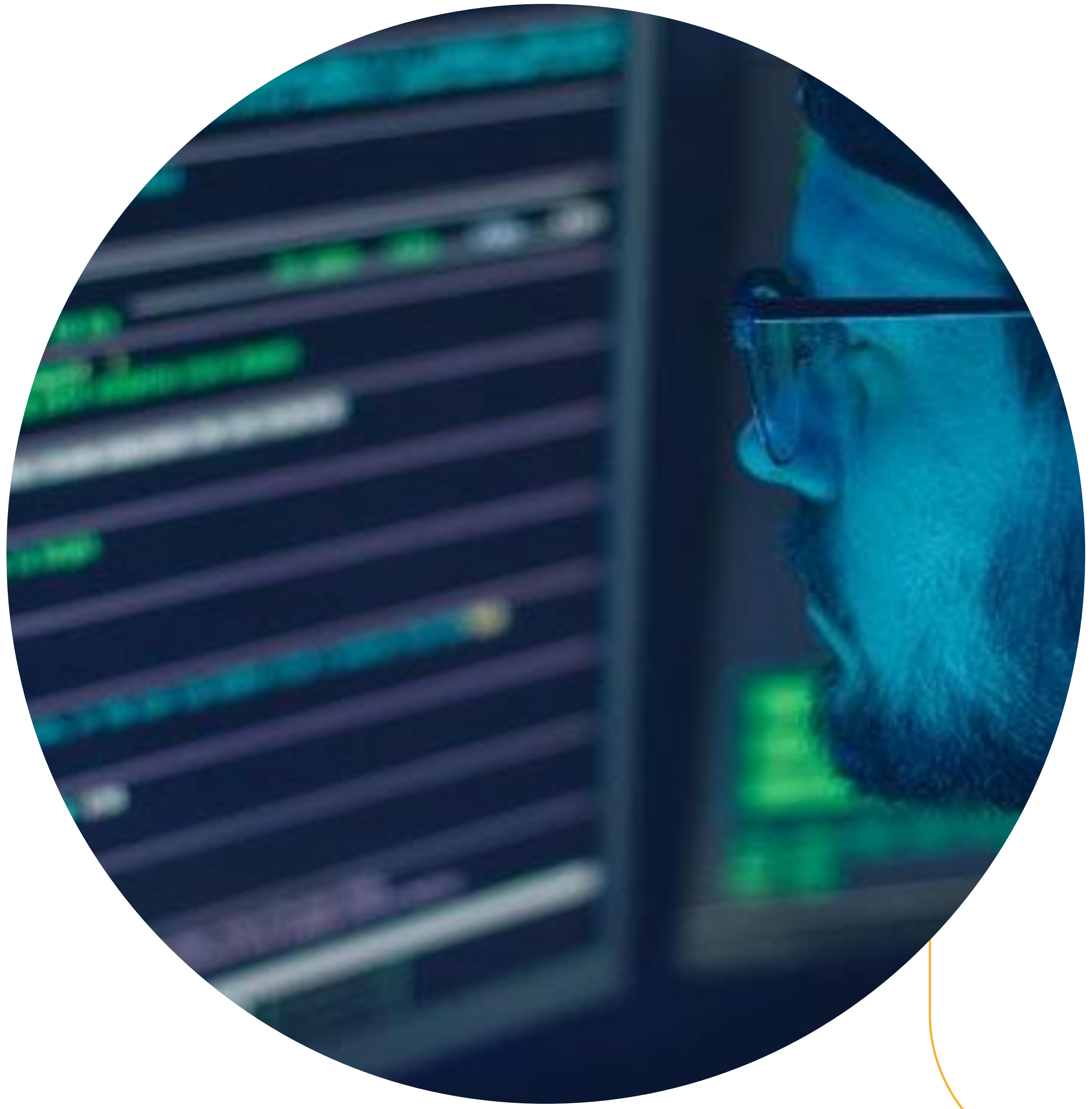
CRYPTOGRAPHIC USES.

Homomorphic encryption.

Homomorphic encryption is a specialized type of encryption that allows data to be analyzed without making the sensitive data visible to the party conducting the analysis.

HIPAA laws, for example, require that patient data be shared only for medical purposes — that doesn't necessarily include statistical analysis, but that information could be quite useful.

Homomorphic encryption permits users to perform analysis without first decrypting the data; the analysis output is nonetheless identical to what would have been produced from unencrypted data.



CRYPTOGRAPHIC USES.

Knowledge check.

Let's apply what we have covered:

- Which IPSec protocol is used when connecting over the internet?
- Describe the two methods of key stretching and what it is used for.

Public Key Infrastructure.

PUBLIC KEY INFRASTRUCTURE.

Key concepts.

In this section, we will cover the following key concepts:

- Public Key Infrastructure (PKI).
- CAs, RAs, Offline, and Online.
- Key Escrow.
- Digital Certificates.
- Lifecycle.
- CRLs and OCSP.
- Certificate Types and Purposes.

PUBLIC KEY INFRASTRUCTURE.

Public Key Infrastructure (PKI).

Public Key Infrastructure (PKI) is built around a server that creates, issues, and stores digital certificates. As the name implies, there is a public key and a private key associated with each digital certificate.

This design offers a number of useful features. The digital certificate provides proof of identity for a person, a website, or a server. The asymmetric keys allow for easy key exchange, either to encrypt with the public key or to use the public key to encrypt a session key for easy exchange.

The hash algorithm and the private key provide digital signatures, which authenticate the source and verify file integrity.

PUBLIC KEY INFRASTRUCTURE.

PKI.

- Certificate authorities (CAs) issue certificates to sites to attest that the site is what it claims to be and verifies the person registering the certificate has legitimate access to the site. The certificates are digitally signed by the CA to validate that they remain unaltered, and they must also tie to the domain for which they attest.
- The CA receives a request for a new certificate and sends the RA to verify the identity of the requester.
- The CA sends the registration authority (RA) to the organization requesting the certificate to ascertain that the request is a legitimate one made by an officer of the organization who was authorized to make the request.

PUBLIC KEY INFRASTRUCTURE.

Offline and online.

Online — The primary CA, known as the root CA, issues certificates and digitally signs them with its own self-signed digital certificate. If the root CA were compromised, the attacker would be able to issue certificates that would appear to be legitimate but were never requested. At this point, any certs issued by the root server would be suspect, as it would be difficult to know which ones were issued by the CA and which were not; as a result, all of the certs, numbering in the thousands potentially, would be revoked, and the legitimate ones would be reissued with a new digital signature.

CAs, other than the root CA, are online at all times to sign certificates.

CONTINUED ON NEXT SLIDE >

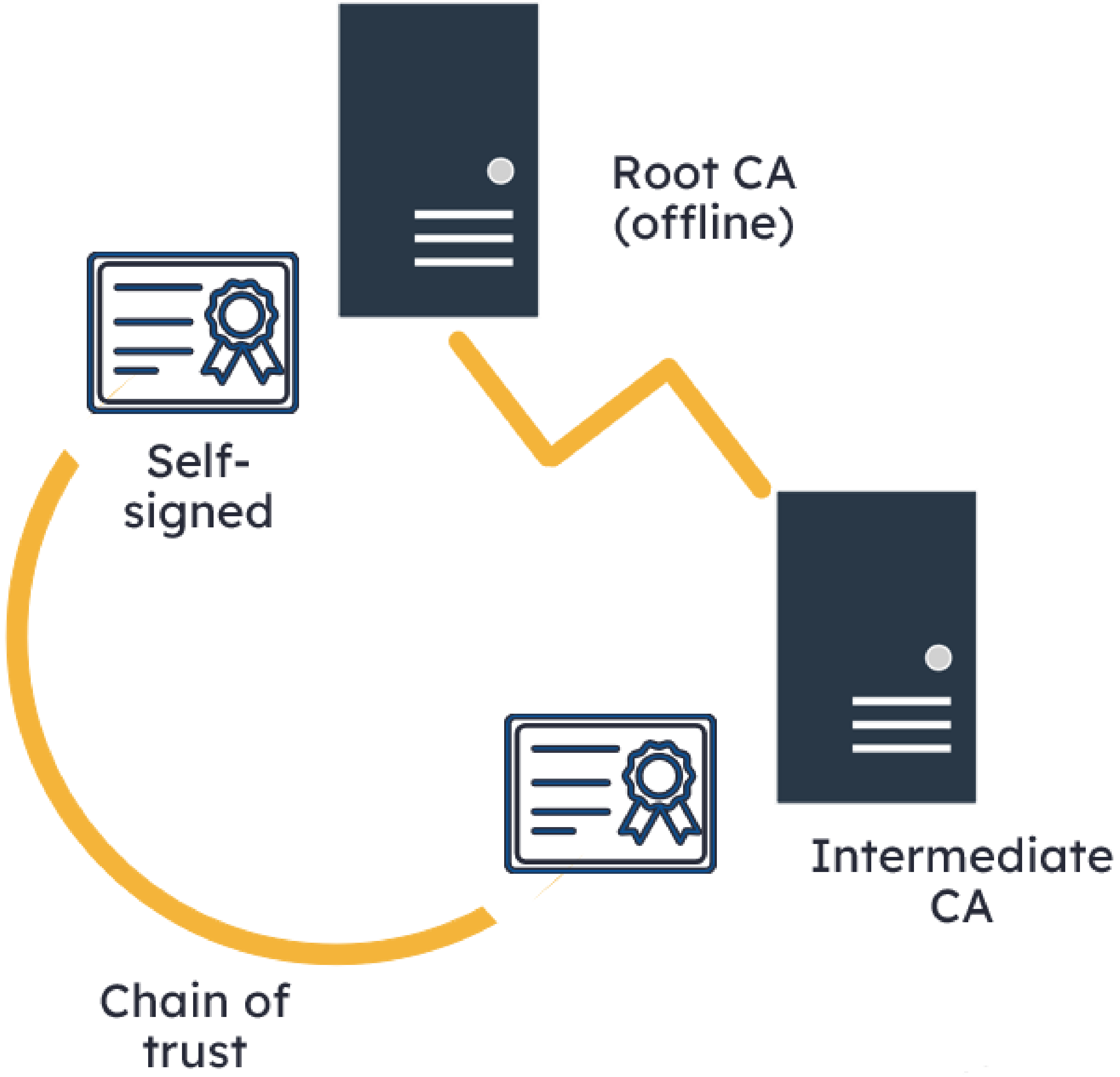
PUBLIC KEY INFRASTRUCTURE.

Offline and online.

Offline — To prevent this scenario, the root CA issues digital certs to several secondary CAs, commonly known as child CAs. The root is then removed from the network and locked away, and the child CAs issue certs as needed, digitally signing them with their own keys. If one of these CAs is compromised, only the certs that CA issued are suspect, not those of the remaining CAs.

PUBLIC KEY INFRASTRUCTURE.

Root and subordinate CA certificates.

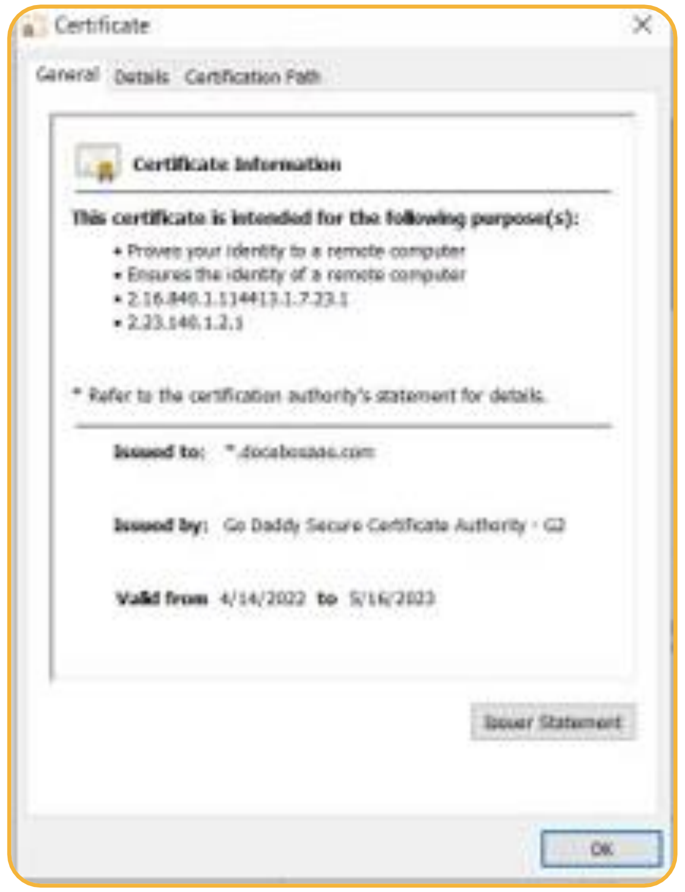


PUBLIC KEY INFRASTRUCTURE.

Digital certificates.

Digital certificates act as a wrapper for the public key and other elements of the credential set, such as the hash algorithm, the thumbprint, and the bulk encryption algorithm.

These details are easily viewed on any secure website by clicking the lock icon in the address bar.



Certificate Information

This certificate is intended for the following purpose(s):

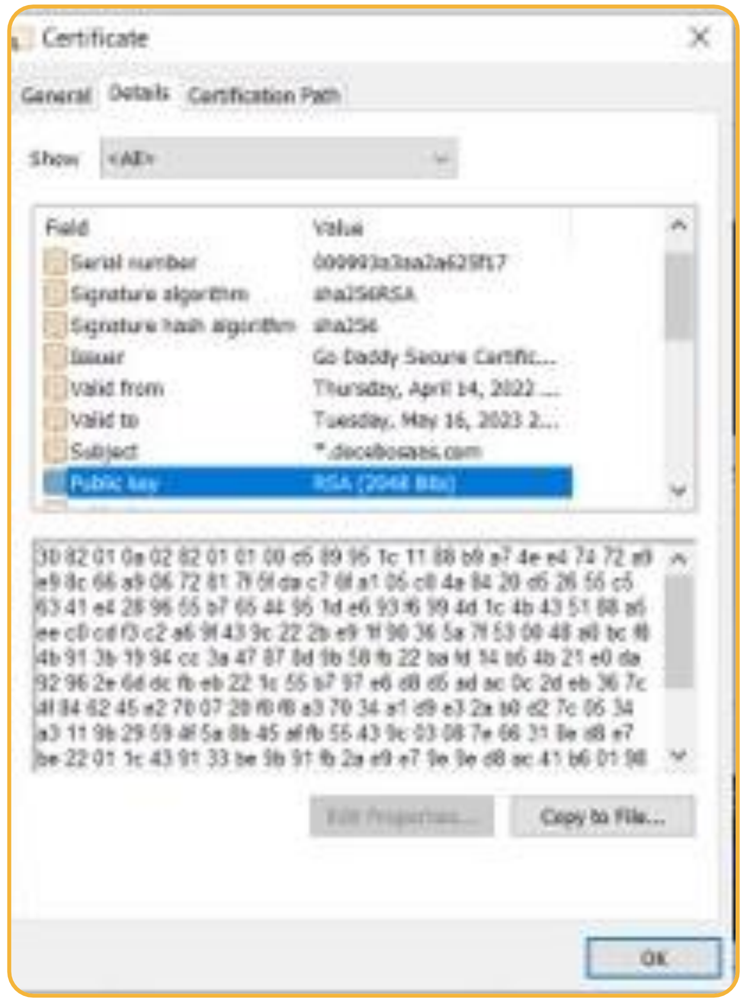
- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.16.840.1.114413.1.7.23.1
- 2.23.140.1.2.1

* Refer to the certification authority's statement for details.

Issued to: *.docebosaas.com

Issued by: Go Daddy Secure Certificate Authority - G2

Valid from 4/14/2022 **to** 5/16/2023



Show <All>

Field	Value
Serial number	000993a3aa2a625f17
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Go Daddy Secure Certific...
Valid from	Thursday, April 14, 2022 ...
Valid to	Tuesday, May 16, 2023 2...
Subject	*.docebosaas.com
Public key	RSA (2048 Bits)

```
30 82 01 0a 02 82 01 01 00 d5 89 95 1c 11 88 b9 a7 4e e4 74 72 a9
e9 8c 66 a9 06 72 81 7f 5f da c7 6f a1 06 c8 4a 84 20 d6 26 55 c5
63 41 e4 28 96 55 b7 65 44 95 1d e6 93 f6 99 4d 1c 4b 43 51 88 a6
ee c0 cd f3 c2 a6 9f 43 9c 22 2b e9 1f 90 36 5a 7f 53 00 48 a0 bc f8
4b 91 3b 19 94 cc 3a 47 87 8d 9b 58 fb 22 ba fd 94 b6 4b 21 e0 da
92 96 2e 6d dc fb eb 22 1c 55 b7 97 e6 d8 d5 ad ac 0c 2d eb 36 7c
4f 84 62 45 e2 70 07 28 f0 f8 a3 70 34 a1 d9 e3 2a b0 d2 7c 06 34
a3 11 9b 29 59 4f 5a 8b 45 af fb 55 43 9c 03 08 7e 66 31 8e d8 e7
be 22 01 1c 43 91 33 be 5b 91 fb 2a e9 e7 9e 9e d8 ac 41 b6 01 98
```

PUBLIC KEY INFRASTRUCTURE.

Key escrow.

Key escrow is a service provided by a company to secure a backup of the keys by the client company to its employees, systems, and websites. A backup set must be maintained against the possibility that the keys might be destroyed or otherwise lost.

However, if the keys used to authenticate users and systems were available to network administrators, they could be used to impersonate the certificate holders.

CONTINUED ON NEXT SLIDE >

PUBLIC KEY INFRASTRUCTURE.

Key escrow.

Non-repudiation is an information security principle that states that your actions should be indisputably tied to you. This is achieved if your credentials, such as your digital cert and its private key, are available only to you. Key escrow allows the backup keys to be stored with a trusted vendor who specializes in this service.

M of N is an associated principle that states keys should be recoverable only by a group of several administrators as a precaution against an abuse of power. M in the minimum number of admins out of the total number (N) of admins — for instance, if three of five authorized admins collectively request the keys, they can recover them together.

PUBLIC KEY INFRASTRUCTURE.

Certificate lifecycle.

The certificate lifecycle describes the certificate process from request to retirement. When a cert is requested, it may or may not be issued. If it is issued, the lifecycle begins.

The lifecycle may be extended by renewing the certificate, with or without new keys being issued. Alternately, the lifecycle may end in several ways, including expiring naturally at its end date.

It may be suspended temporarily but can be reinstated as long as it hasn't expired.

CONTINUED ON NEXT SLIDE >

PUBLIC KEY INFRASTRUCTURE.

Certificate lifecycle.

- It may be revoked early for various reasons, such as selling off the portion of the company using the cert, because the user is leaving, perhaps because the cert is no longer needed, or if it is compromised.

  Any of the last three states means the certificate is invalid and should not be trusted.

PUBLIC KEY INFRASTRUCTURE.

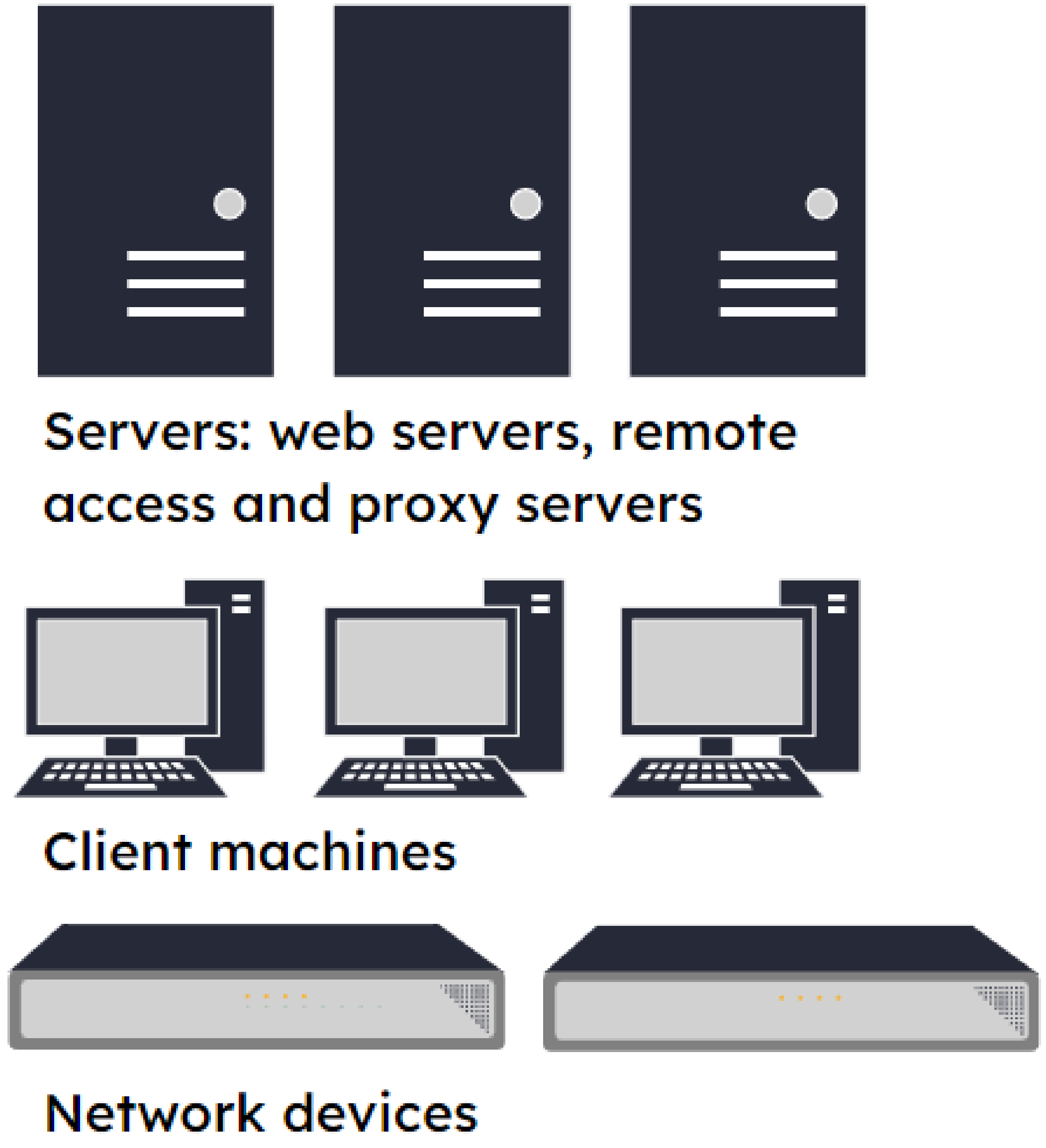
Certificate revocation lists (CRLs).

Certificate revocation lists (CRLs) hold records for each certificate that has expired, been revoked, or been suspended. Over time, these lists can get quite large. Because multiple CAs may be involved, each with different certs, this information is periodically shared from CA to CA; however, between updates, one CA may be unaware that a cert has been revoked a CA it issued.

PUBLIC KEY INFRASTRUCTURE.

OCSP and machine certificates.

Online Certificate Status Protocol (OCSP) is used to enquire about a single cert. A CA being presented with a cert that was issued by another related CA in the same organization would send a query as to the status of that cert; the issuing CA would respond with the cert's current status.



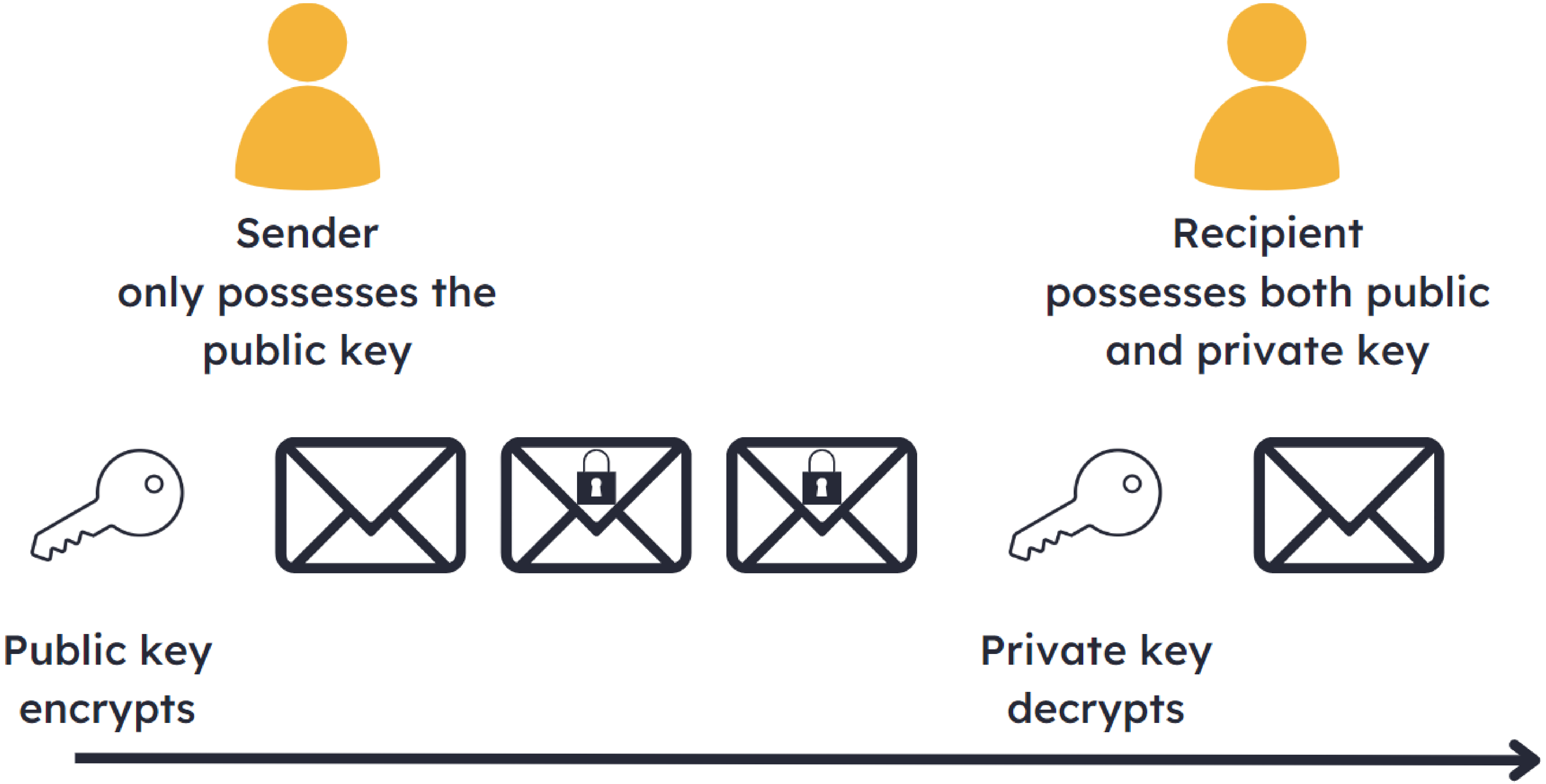
PUBLIC KEY INFRASTRUCTURE.

User certificates.

- Email.
- Disk encryption.
- Identity to remote users/computers.

PUBLIC KEY INFRASTRUCTURE.

Email certificates S/MIME.



Sender
only possesses the
public key

Recipient
possesses both public
and private key

Public key
encrypts

Private key
decrypts

PUBLIC KEY INFRASTRUCTURE.

Code signing certificate.

- Proves the identity of the vendor.
- Ensures integrity of the software via digital signature.
- Operating systems use for validation.

PUBLIC KEY INFRASTRUCTURE.

Wildcard certificate.

- Used to identify a parent domain.
- Verifies all first-level sub (child) domains.
- Represented by an asterisk.
- (*.acilearning.com)

PUBLIC KEY INFRASTRUCTURE.

Validation certificates.

Domain Validation (DV):

- Lowest level of validation.
- Verifies ownership over the domain.

Organization Validation (OV):

- Greater validation than DV.
- Verifies the identity of the organization.

Extended Validation (EV):

- Highest form of organization identification.
- Most rigorous validation process.

Individual Validation (IV):

- Verifies the identity of the individual.

PUBLIC KEY INFRASTRUCTURE.

Certificate formats and purpose.

Distinguished Encoding Rules (DER):

- Binary encoded.
- Does not include private keys.
- (.cer)

Privacy Enhanced Mail (PEM):

- Base64 ASCII encoded.
- Various extensions (.pem, .cer, .crt)

Public Key Cryptography Standards #7 (PKCS#7):

- Includes public key, certificate information, and certificate chain.
- (.P7B)

Public Key Cryptography Standards #12 (PKCS#12):

- Includes both public/private keys and certificate information. (includes extended properties), and certificate chain.

PUBLIC KEY INFRASTRUCTURE.

Knowledge check.

Let's apply what we have covered:

- Describe the differences in cert validation.
- Describe the function of PKI.

End of Module.

For additional practice, please complete all associated self-study activities and labs.