Security

A-Level Computer Science · Vocabulary in context

Word	Example
encryption /enˈkrɪpʃn/	**Encryption** makes the message unreadable to others.
plaintext /ˈpleɪntekst/	The message before encryption is **plaintext**.
ciphertext /ˈsaɪfətekst/	The encrypted message is **ciphertext**.
decryption /dɪˈkrɪpʃn/	**Decryption** turns ciphertext back into plaintext.
quantum cryptography /ˈkwɒntəm krɪpˈtɒgrəfi/	**Quantum cryptography** uses light to share keys.
eavesdropper /ˈiːvzdrɒpə/	An **eavesdropper** tries to read the message.
symmetric encryption /sɪˈmetrɪk enˈkrɪpʃn/	**Symmetric encryption** uses one key for both sides.
key distribution /kiː ˌdɪstrɪˈbjuːʃn/	**Key distribution** is how the key reaches the other person.
asymmetric encryption /ˌeɪsɪˈmetrɪk enˈkrɪpʃn/	**Asymmetric encryption** uses a public key and a private key.
integrity /ɪnˈtegrɪti/	Data **integrity** means the data is correct and complete.
public key /ˈpʌblɪk kiː/	Anyone can use your **public key**.
private key /ˈpraɪvət kiː/	Keep your **private key** secret.
digital signature /ˈdɪdʒɪtl ˈsɪgnɪtʃə/	A **digital signature** proves who sent the message.

exercises.lol exercises.com.cn

Word	Example
hardware security key /ˈhɑːdweə sɪˈkjʊərɪti kiː/	A **hardware security key** plugs into the computer to log in.
session key /ˈseʃn kiː/	A new **session key** is made for each visit.
cryptographic hash /ˌkrɪptəˈgræfɪk hæʃ/	A **cryptographic hash** is easy to make but hard to undo.
digest /ˈdaɪdʒest/	The hash function gives a short **digest** of the message.
TLS /ˌtiː el ˈes/	**TLS** keeps your bank website safe.
authentication /ɔːˌθentɪˈkeɪʃn/	A password is a kind of **authentication**.
authenticates /ɔːˈθentɪkeɪts/	The certificate **authenticates** the website.
handshake /ˈhændʃeɪk/	The **handshake** sets up the secure link.
digital certificate /ˈdɪdʒɪtl səˈtɪfɪkət/	A **digital certificate** proves that the website is real.
Certificate Authority /səˈtɪfɪkət əˈθɒrɪti/	A **Certificate Authority** gives out digital certificates.
man-in-the-middle /mæn ɪnðə ˈmɪdl/	In a **man-in-the-middle** attack, someone reads messages between two people.