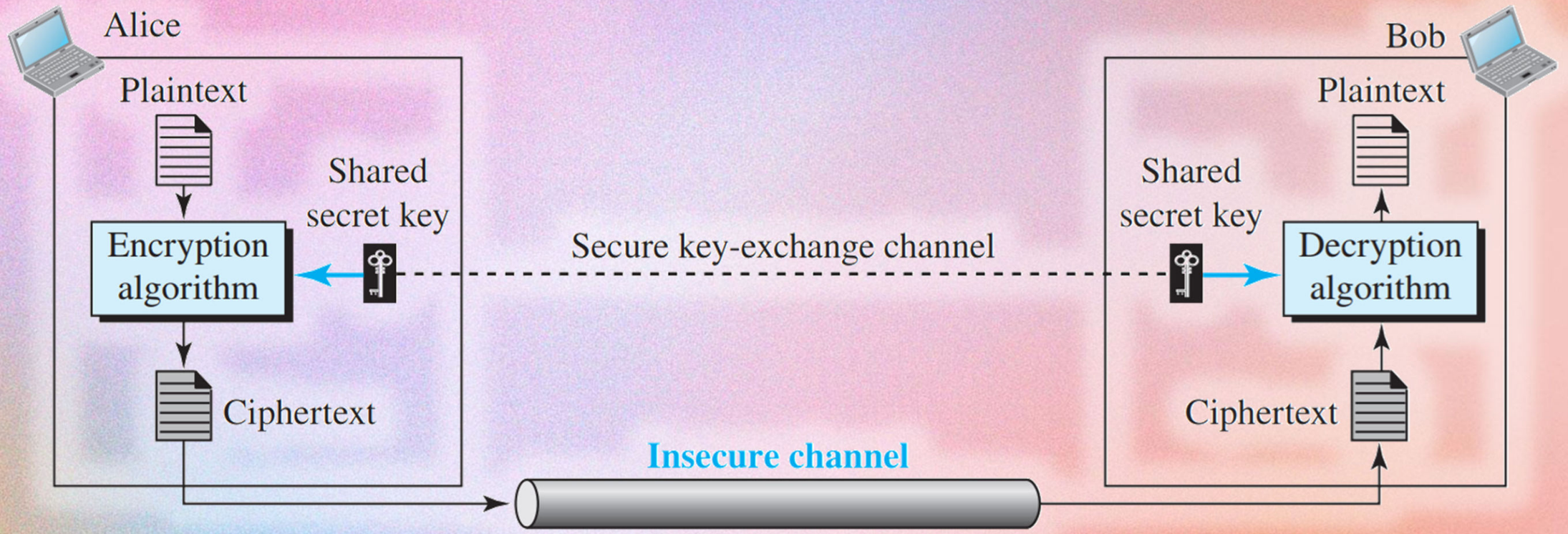
CRYPTOGRAPHIC PROTOCOLS

INFORMATION SECURITY VS. CRYPTOGRAPHY

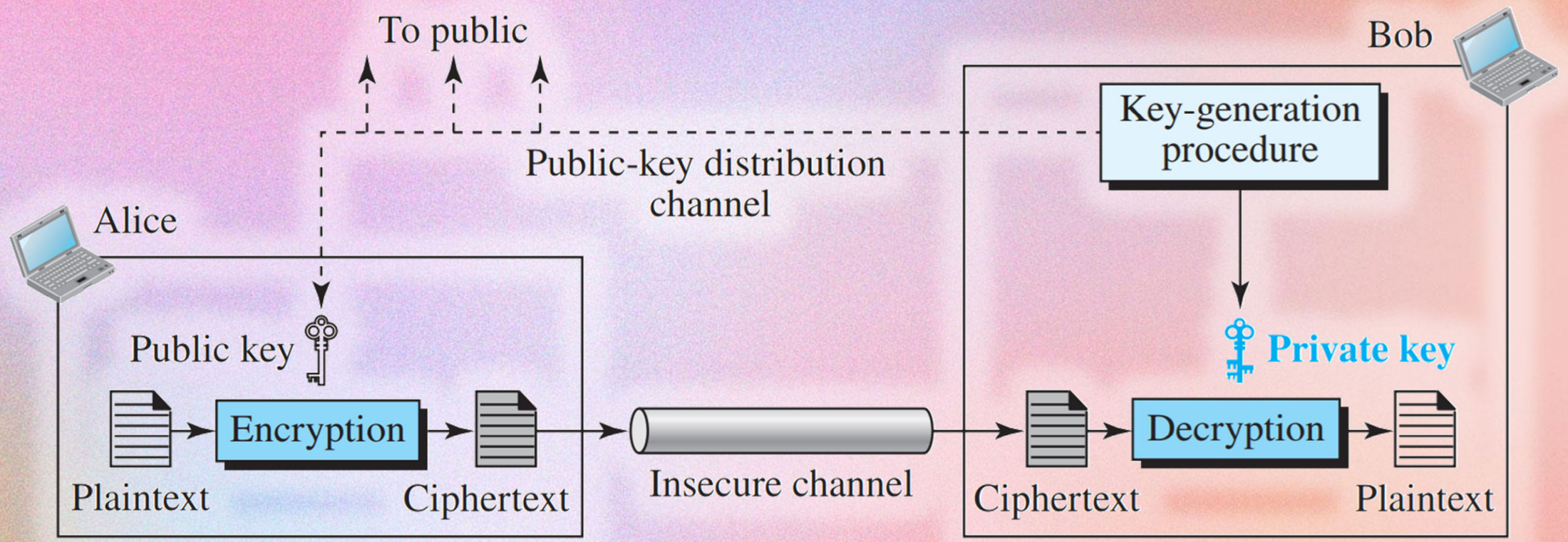
Information Security		Cryptography	
Confidentiality	Parties **cannot access data they're not authorized** to access.	**Encryption Algorithms**	Performs the **transformation of data into ciphertext.**
Integrity	All information contained within company databases is **complete and accurate.**	**Hash Functions**	Transforms an input into **a string of characters of a fixed length.**
		Digital Signature	A **message digest encrypted with the message sender's private key.**

https://www.ibm.com/think/topics/cryptography
https://www.ibm.com/think/topics/information-security
https://www.ibm.com/docs/en/cics-ts/5.6?topic=protection-digital-signatures

SYMMETRIC-KEY CIPHER



ASYMMETRIC-KEY CIPHER



Data Encryption Standard

Advanced Encryption Standard

MODERN ASYMMETRIC-KEY CIPHERS

RSA

ECC

INFORMATION SECURITY VS. CRYPTOGRAPHY

Information Security		Cryptography	
Confidentiality	Parties **cannot access data they're not authorized** to access.	**Encryption Algorithms**	Performs the **transformation of data into ciphertext.**
Integrity	All information contained within company databases is **complete and accurate.**	**Hash Functions**	Transforms an input into **a string of characters of a fixed length.**
		Digital Signature	A **message digest encrypted with the message sender's private key.**

https://www.ibm.com/think/topics/cryptography
https://www.ibm.com/think/topics/information-security
https://www.ibm.com/docs/en/cics-ts/5.6?topic=protection-digital-signatures

Hash functions are essential in cryptography because they allow you to **verify data without exposing the original content.**

COMMONLY USED CHFs

Hash Function	Output Length (bits)	Common Applications
MD5	128	File integrity checking, older systems, non-crypto uses
SHA-1	160	Legacy systems, Git for version control
SHA-256	256	Cryptocurrency (Bitcoin), digital signatures, certificates
SHA-3	Variable (up to 512)	Various cryptographic applications, successor to SHA-2
Blake2	Variable (up to 512)	Cryptography, replacing MD5/SHA-1 in some systems
Blake3	Variable (up to 256)	Cryptography, file hashing, data integrity

INFORMATION SECURITY VS. CRYPTOGRAPHY

Information Security		Cryptography	
Confidentiality	Parties **cannot access data they're not authorized** to access.	**Encryption Algorithms**	Performs the **transformation of data into ciphertext.**
Integrity	All information contained within company databases is **complete and accurate.**	**Hash Functions**	Transforms an input into **a string of characters of a fixed length.**
		Digital Signature	A **message digest encrypted with the message sender's private key.**

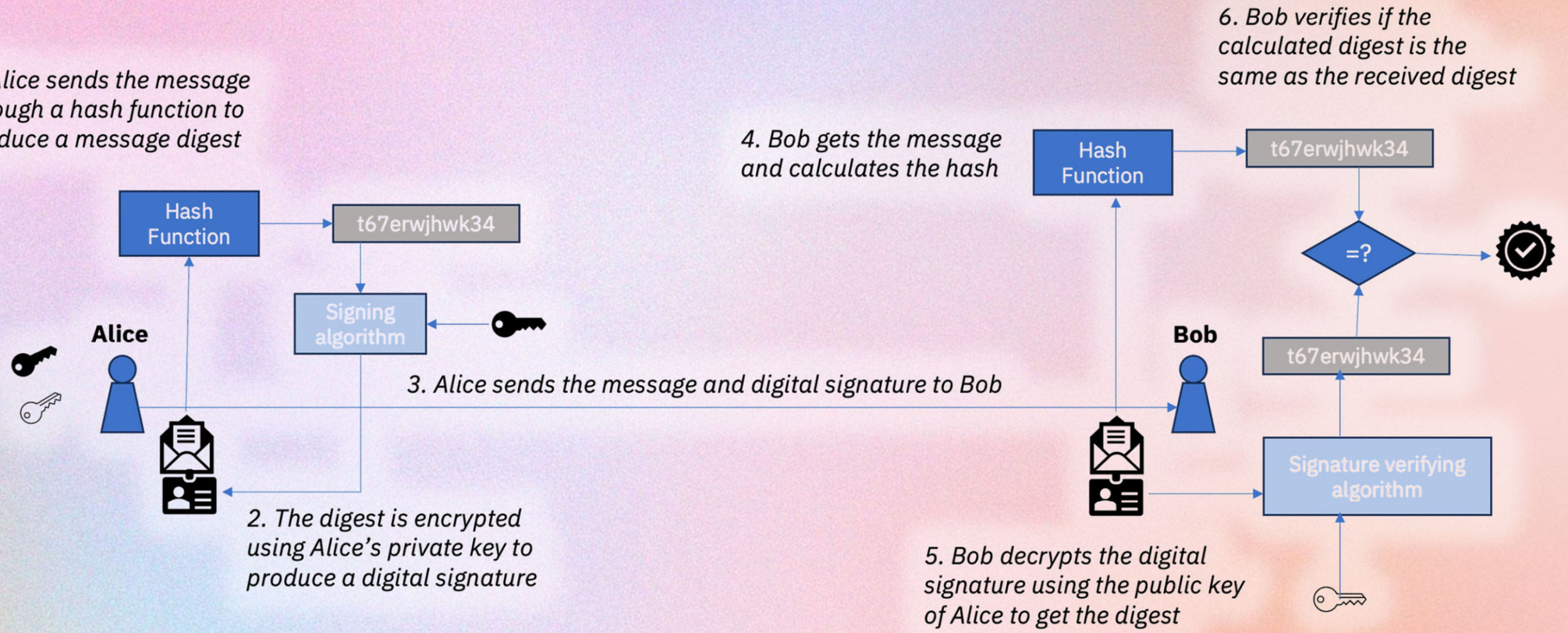
https://www.ibm.com/think/topics/cryptography
https://www.ibm.com/think/topics/information-security
https://www.ibm.com/docs/en/cics-ts/5.6?topic=protection-digital-signatures

INFORMATION SECURITY VS. CRYPTOGRAPHY

Information Security		Cryptography	
Nonrepudiation	A user **cannot deny having made a transaction.**	**Digital Signature**	**A message digest encrypted with the message sender's private key.**

https://www.ibm.com/think/topics/cryptography
https://www.ibm.com/think/topics/information-security
https://www.ibm.com/docs/en/cics-ts/5.6?topic=protection-digital-signatures

DIGITAL SIGNATURES



Now that we understand the core building blocks of cryptography, such as encryption algorithms, hash functions, and digital signatures.

We can explore how these elements work together to enable secure communication.

This is where **cryptographic protocols** come into play.

We can explore how these elements work together to enable secure communication.

This is where **cryptographic protocols** come into play.

PROTOCOL

A **system of rules** that explain the correct conduct and procedures to be followed in formal situations.

Content Curated by Pollux M. Rey

https://www.britannica.com/dictionary/eb/qa/what-does-protocol-mean

Content Curated by Pollux M. Rey

CRYPTOGRPHIC PROTOCOL

Consist of **rules and procedures that use cryptographic algorithms** to secure communication and protect data.

Content Curated by Pollux M. Rey

https://www.ssl.com/article/what-is-a-cryptographic-protocol/

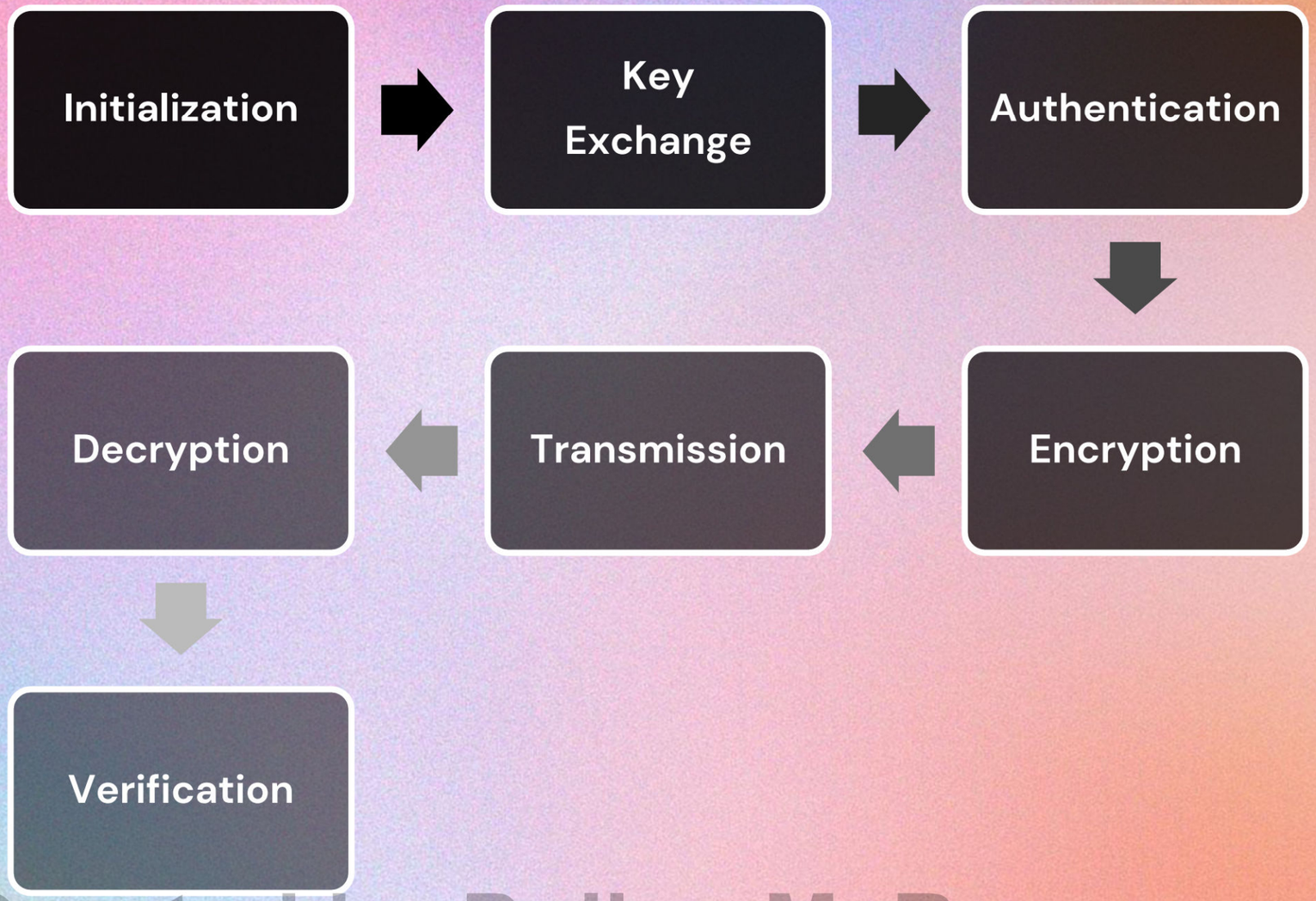
PURPOSE

The primary purposes of cryptographic protocols include:

1. **Confidentiality:** Ensuring that only authorized parties can access the information
2. **Integrity:** Guaranteeing that the information has not been altered during transmission
3. **Authentication:** Verifying the identity of the parties involved in the communication
4. **Non-repudiation:** Preventing parties from denying their involvement in a transaction

https://www.ssl.com/article/what-is-a-cryptographic-protocol/

HOW CRYPTOGRAPHIC PROTOCOLS WORK



https://www.ssl.com/article/what-is-a-cryptographic-protocol/

INITIALIZATION

The parties involved **agree on the protocol and necessary parameters**.

https://www.ssl.com/article/what-is-a-cryptographic-protocol/

KEY EXCHANGE

A secure method is used to exchange encryption keys.

https://www.ssl.com/article/what-is-a-cryptographic-protocol/

KEY EXCHANGE PROTOCOLS

1. **Diffie-Hellman Key Exchange**: Allows two parties to establish a **shared secret key** over an insecure channel
2. **RSA Key Exchange**: Uses the RSA algorithm for secure key exchange

https://www.ssl.com/article/what-is-a-cryptographic-protocol/

AUTHENTICATION

The identities of the parties are verified.

https://www.ssl.com/article/what-is-a-cryptographic-protocol/

AUTHENTICATION PROTOCOLS

1. **Kerberos**: A network authentication protocol that uses tickets to allow nodes to prove their identity
2. **OAuth**: An open standard for access delegation, commonly used for secure API authentication

https://www.ssl.com/article/what-is-a-cryptographic-protocol/

ENCRYPTION

Data is encrypted using the agreed-upon algorithms and keys.

https://www.ssl.com/article/what-is-a-cryptographic-protocol/

ENCRYPTION

Data is encrypted using the agreed-upon algorithms and keys.

https://www.ssl.com/article/what-is-a-cryptographic-protocol/

TRANSMISSION

The encrypted data is sent over the network.

https://www.ssl.com/article/what-is-a-cryptographic-protocol/

DECRYPTION

The recipient decrypts the data using their key.

https://www.ssl.com/article/what-is-a-cryptographic-protocol/

VERIFICATION

The integrity and authenticity of the received data are checked.

https://www.ssl.com/article/what-is-a-cryptographic-protocol/

DIGITAL SIGNATURE PROTOCOLS

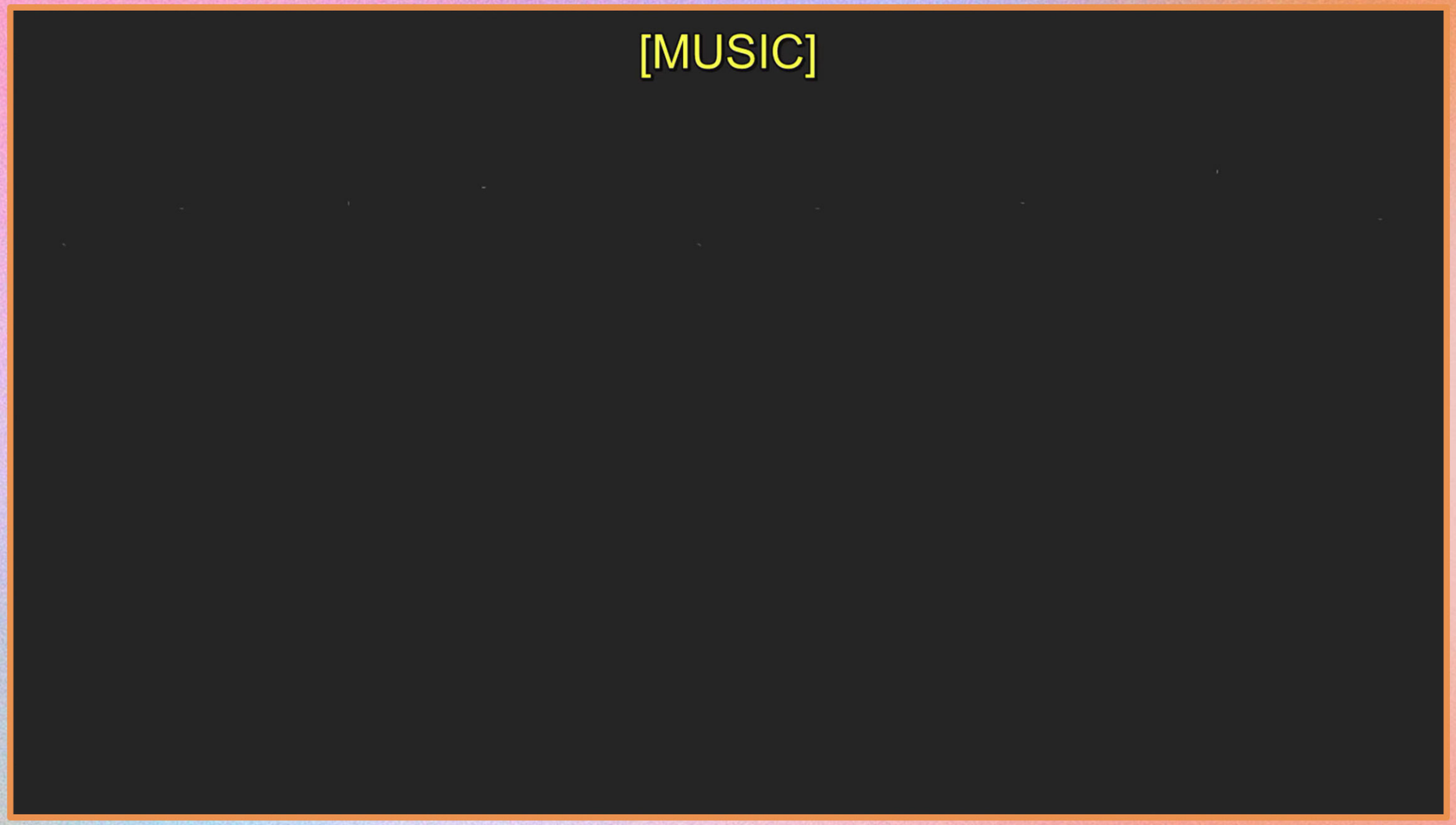
1. **DSA (Digital Signature Algorithm)**: A federal government standard for digital signatures
2. **ECDSA (Elliptic Curve Digital Signature Algorithm)**: A variant of DSA using elliptic curve cryptography

https://www.ssl.com/article/what-is-a-cryptographic-protocol/

The cryptographic protocol most internet users are familiar with is the Secure Sockets Layer (or SSL) protocol, with its descendant the **Transport Layer Security (or TLS) protocol**.

Content Curated by Pollux M. Rey

https://www.ssl.com/article/what-is-a-cryptographic-protocol/



https://www.youtube.com/watch?v=j9QmMEWmcfo

IMPORTANCE OF CRYPTOGRAPHIC PROTOCOLS

1. **Protecting sensitive information**: They safeguard personal, financial, and confidential data from unauthorized access.
2. **Enabling secure e-commerce**: Protocols like SSL/TLS make online transactions secure, fostering trust in digital commerce.
3. **Ensuring privacy**: They protect communications from eavesdropping and interception.
4. **Verifying identities**: Authentication protocols help prevent impersonation and fraud in digital interactions.
5. **Compliance with regulations**: Many industries require the use of cryptographic protocols to meet data protection standards.

https://www.ssl.com/article/what-is-a-cryptographic-protocol/

THANK YOU!

Content Curated by Pollux M. Rey