An Introduction to Cryptography Concepts for Developers

Introduction

Cryptography is essential for securing sensitive data. This introduction covers basic cryptography concepts every developer should know.

Cryptography Basics

- Encryption converts data to ciphertext that is unreadable without a key.
- Hashing creates a unique fixed-length string fingerprint from input.
- Digital signatures enable identity verification and document authentication.
- Key exchange allows securely sharing keys for encryption.

Encryption Algorithms

- Symmetric algorithms use the same key to encrypt and decrypt.
- Asymmetric algorithms use a public/private key pair.
- Common algorithms: AES, RSA, Blowfish, RC4, ECC.

Hashing Algorithms

- SHA-2, SHA-3, MD5, etc take variable length input and output fixed length hashes.
- Important uses include verifying data integrity and securing passwords

Use Cases

- Encrypting data at rest and in transit.
- Storing passwords and sensitive data securely.
- Establishing trusted connections.
- Preventing tampering, mitigating MITM attacks.

Conclusion

Understanding cryptography helps developers implement critical security measures in applications.