Cryptography

A field focusing on secure communication, ensuring confidentiality, authenticity, and data integrity. Methods like AES, RSA, and digital signatures are used to encrypt data, authenticate users, and detect tampering

Diffie-Hellman Key Exchange

A cryptographic protocol that allows two parties to securely create a shared secret key over a public channel, relying on the difficulty of solving discrete logarithms.

RSA encryption

A public-key encryption algorithm where large prime numbers are used to generate keys for secure data transmission. The RSA process involves key generation, encryption, and decryption through modular arithmetic.

Breaking RSA

Explains the process of breaking RSA encryption by factoring the modulus into prime numbers and , revealing the private key. It demonstrates the vulnerability of RSA if large primes can be factored.

Digital Signature

A cryptographic method using asymmetric keys to verify the authenticity and integrity of a document. It ensures authenticity, non-repudiation, and that the document has not been tampered with. RSA is one simple method used for digital signatures.

Hash functions

Special functions producing fixed-length outputs from variable inputs, ensuring properties like pre-image and collision resistance. They are essential for digital signatures, password storage, and data integrity.

Digital Signature with Hash code

Combines hashing and encryption, where a document’s hash is encrypted with a private key to create a signature. The recipient verifies it by comparing the decrypted hash with a computed one, ensuring integrity and authenticity.

Public Key Authentication

Prevents man-in-the-middle attacks by using a trusted third party, a Certificate Authority (CA), to authenticate public keys. The CA issues a certificate containing the digital signature, ensuring the key's authenticity and integrity.