Cryptography

```
module = Module(
    code="ELEE1171",
    name="Securing Technologies",
    credits=15,
    module_leader="Seb Blair BEng(H) PGCAP MIET MIHEEM FHEA"
)
```

UNIVERSITY OF GREENWICH

Download as a PDF

Main Goals of Security: CIA

CIA Triad (Information Security)

Confidentiality (C): Ensures that sensitive information is only accessible to authorized individuals, preventing unauthorized access or disclosure.

Integrity (I): Maintains the accuracy and trustworthiness of data by preventing unauthorized modifications.

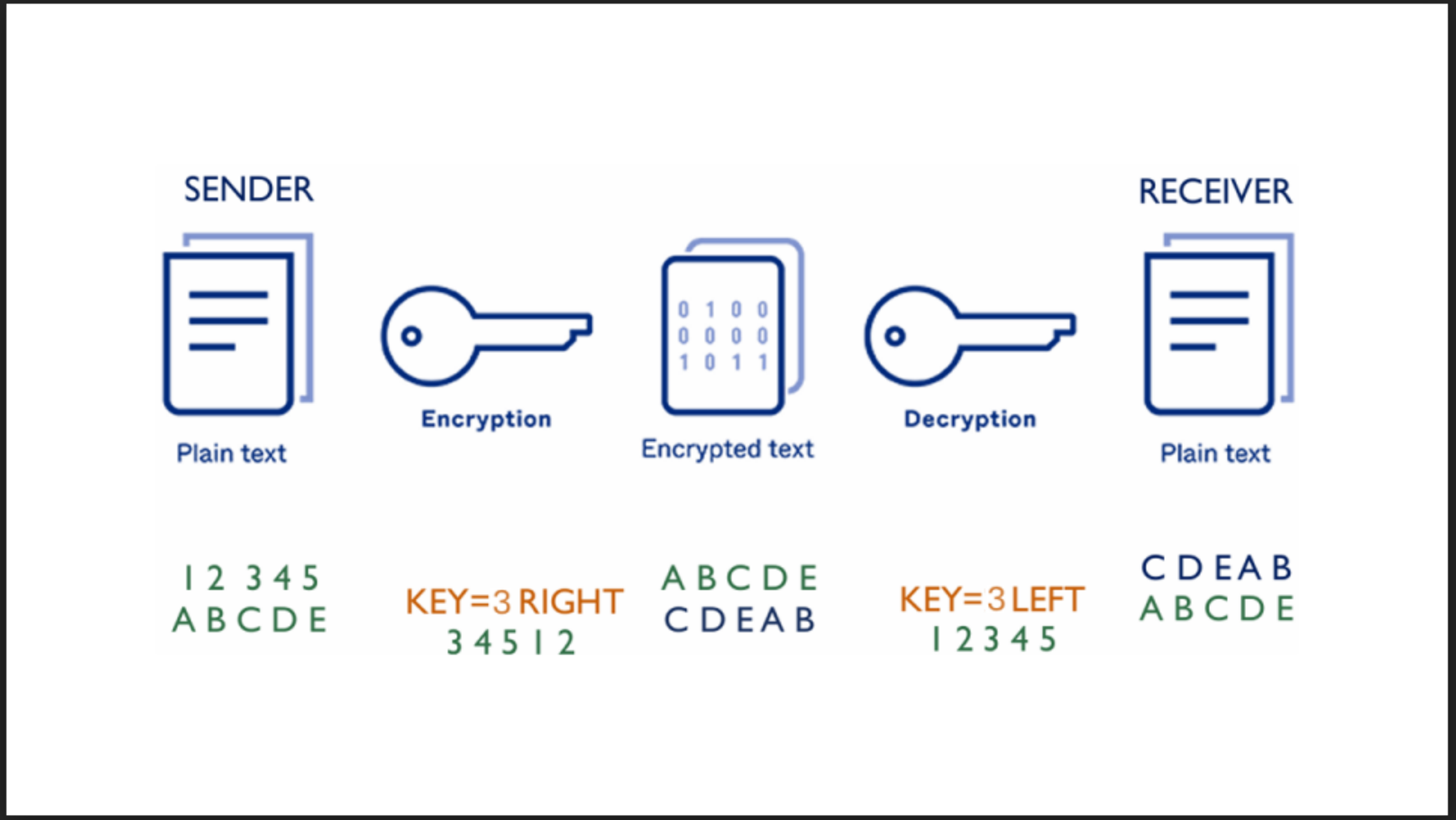
Availability (A): Guarantees that information and systems are accessible to users when needed, ensuring reliable access.

Quick Definitions

- **Cryptography**: the art of secret writing!
- **Encryption**: converting information to a format **unreadable by unintended recipients**. Only intended recipients with the correct key and algorithm can read it and get its true meaning.
- **Hashing**: converts data or message into an irreversible string of fixed length.
- Confidentiality can be achieved using **Encryption**
- Data Integrity can be verified using **Hashing**

Why Do We Need Cryptography?

Encryption - Substitution Cipher



*Also known as Ceaser Cipher

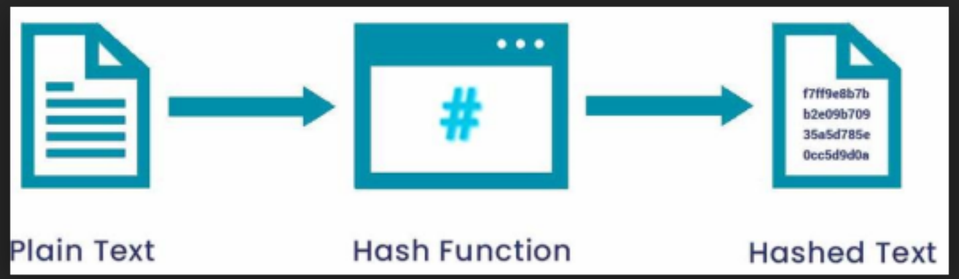
Hashing

Windows

```
certutil-hashfile <filename>    <md5, sha1, sha256, sha512>    [ENTER]
```

Linux/macOS

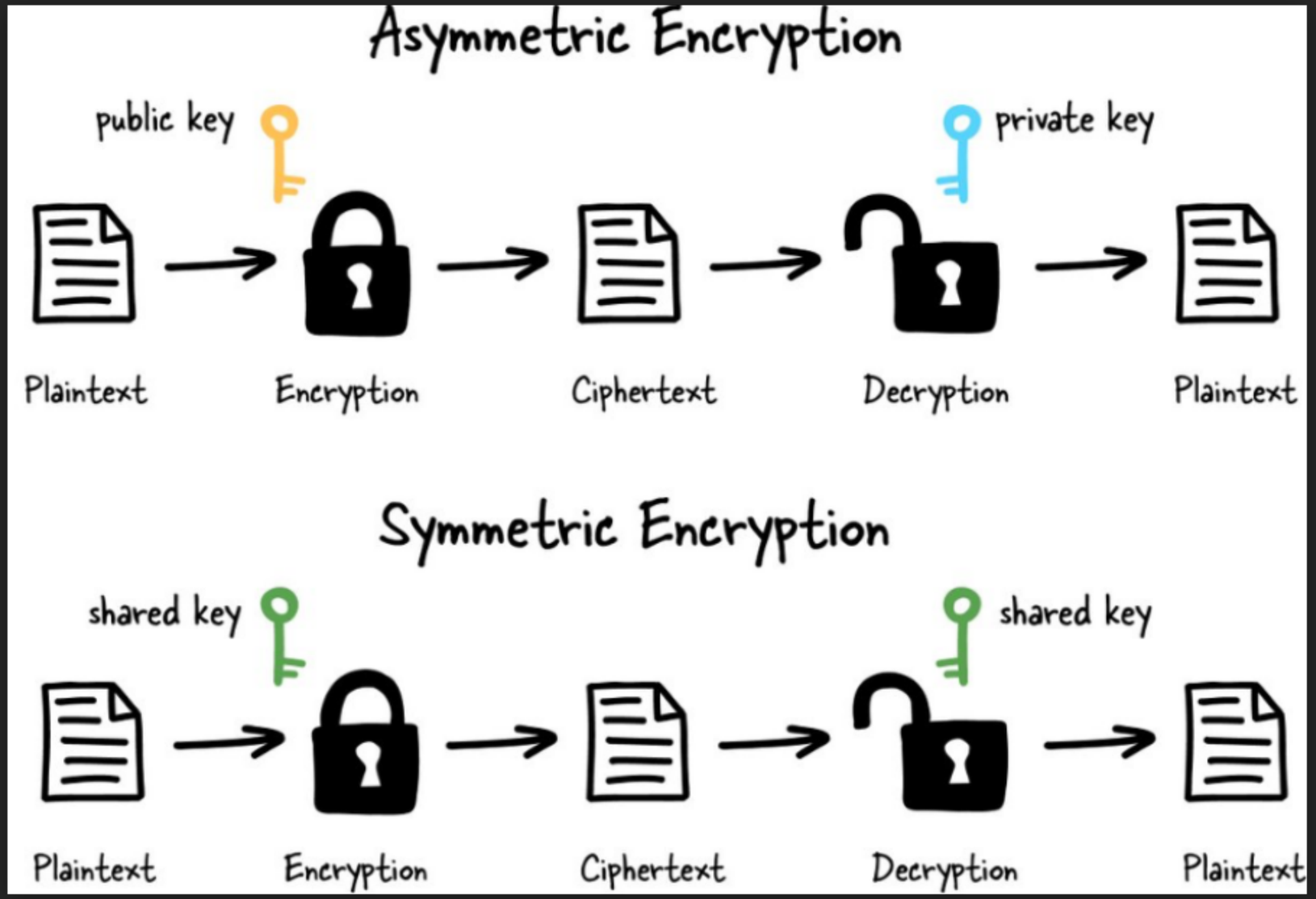
```
sha256sum    <filename>    [ENTER]
```



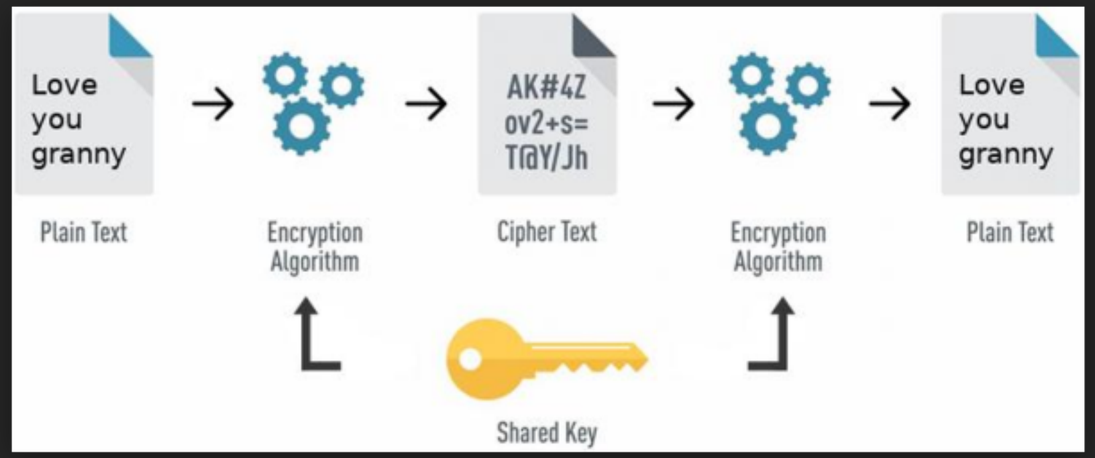
The major difference between Hashing and Encryption is that:

- No keys are used in hashing but only algorithms e.g., MD5

Types of Encryption



Symmetric



- Same key for encryption
- Key sharing is a problem
- Low overhead
- Fast
- Sutiable for transmitting bluk data

Asymmetric

- Uses Public Key Infrastructure (PKI)
- Both parties have their key pair
- One key for encryption, another for decryption
- Solves the problem of key sharing
- High overhead
- No need to/and never share your private key

Example Asymetric

Generate Key

```
$ ssh-keygen -t ed25519 -C "ELEE1171"
```

Public key

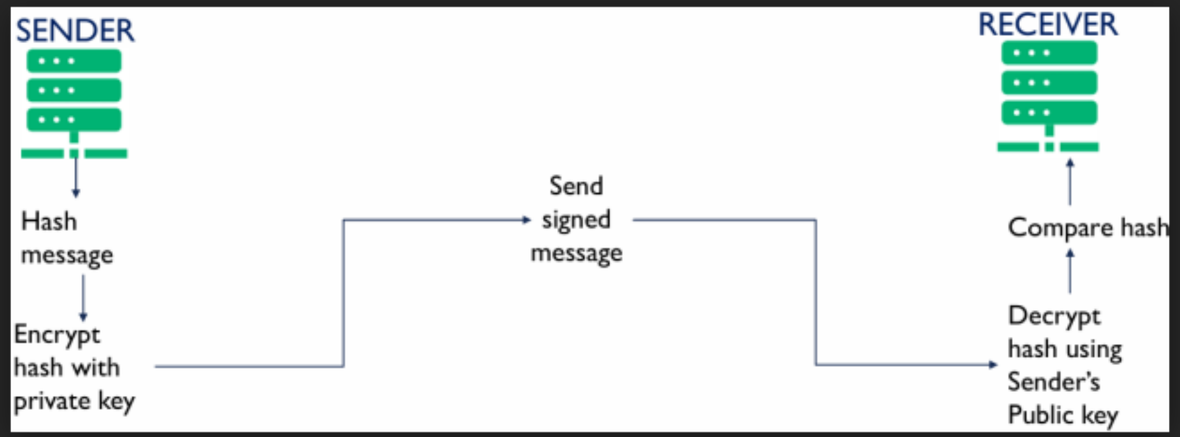
```
cat ~/.ssh/id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJqFxk/iuYfO2GeOx4BTK4Gy0Mhe1g7SQYmQRYnqu3zP ELEE1171
```

Private Key

```
cat ~/.ssh/id_ed25519
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACCahcZP4rmHzthnjseAUyuBstDIXtYO0kGJkEWJ6rt8zwAAAJDGb9KYxm/S
mAAAAAtzc2gtZWQyNTUxOQAAACCahcZP4rmHzthnjseAUyuBstDIXtYO0kGJkEWJ6rt8zw
AAAED0Oks/Py0THM2cX0k+QqhjzGx4CZ6xXU3UL3vejLTHRJqFxk/iuYfO2GeOx4BTK4Gy
0Mhe1g7SQYmQRYnqu3zPAAAACEVMRUUxMTcxAQIDBAU=
-----END OPENSSH PRIVATE KEY-----
```

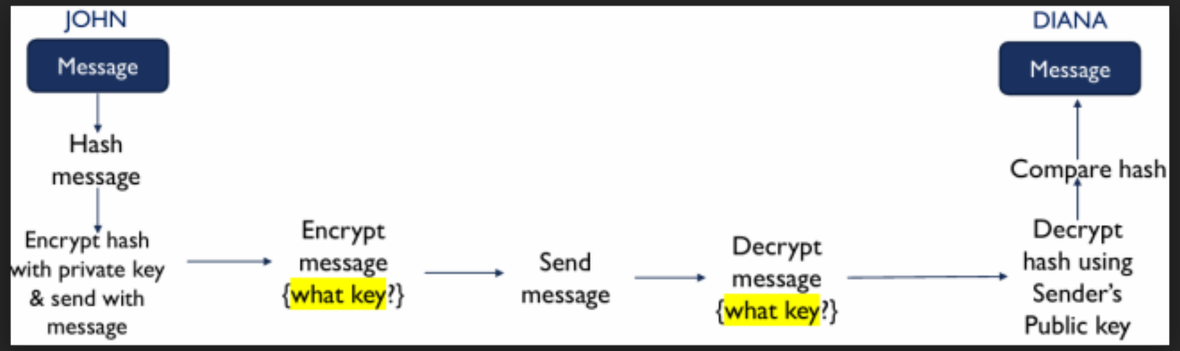
Digital Signature

- Digital Signature:
  - Encrypt message hash with private key, and recipient decrypts hash using sender’s public key.
  - This verifies **authenticity**



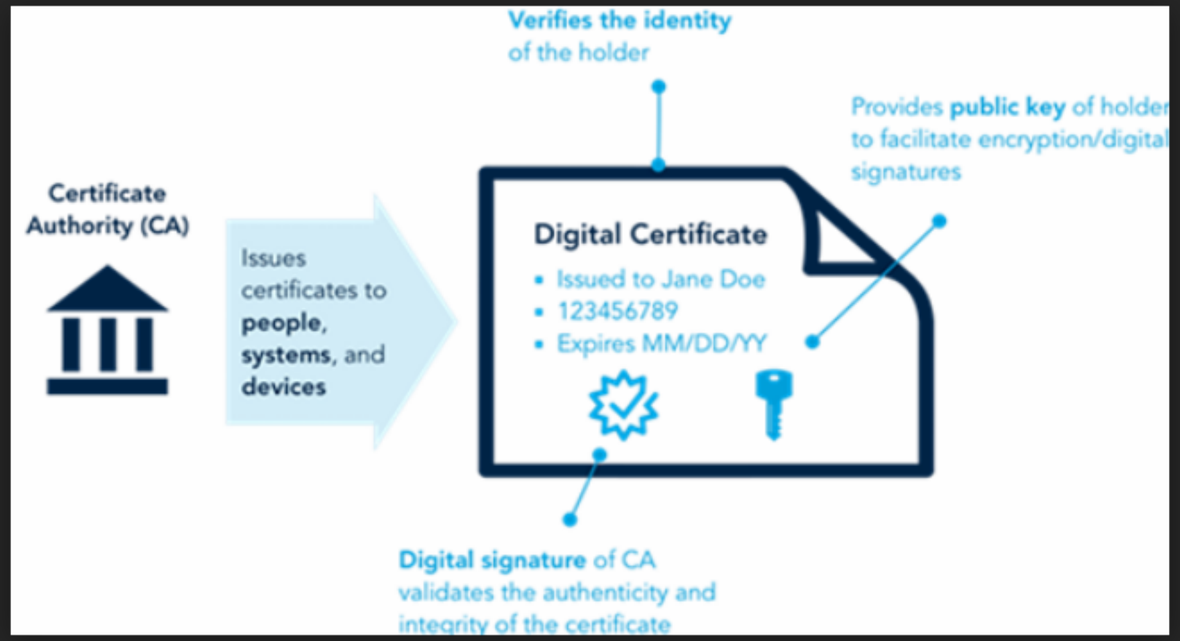
Combining Digital Signature With PKI

- Digital Signature: Encrypt message hash with private key, and recipient decrypts hash using sender's public key. This verifies **authenticity**



Digital Certifcates

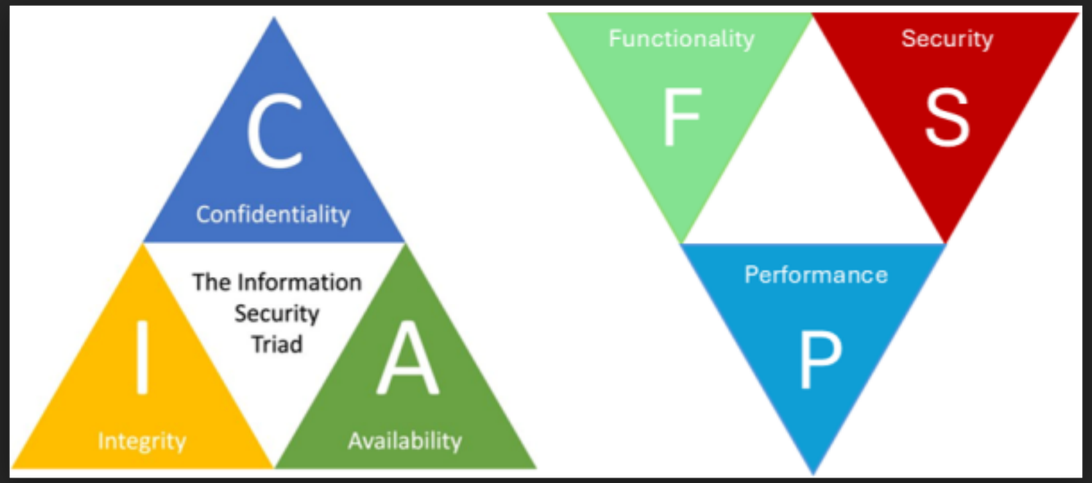
- Digital Certificate: A file that contains your public key and other necessary information to verify the validity and authenticity of your public key.
- Issued by the Certificate Authority (CA)
- A digital certificate is issued after verification of the website or Organisation.
- This is the mechanism your browser uses to detect secure websites



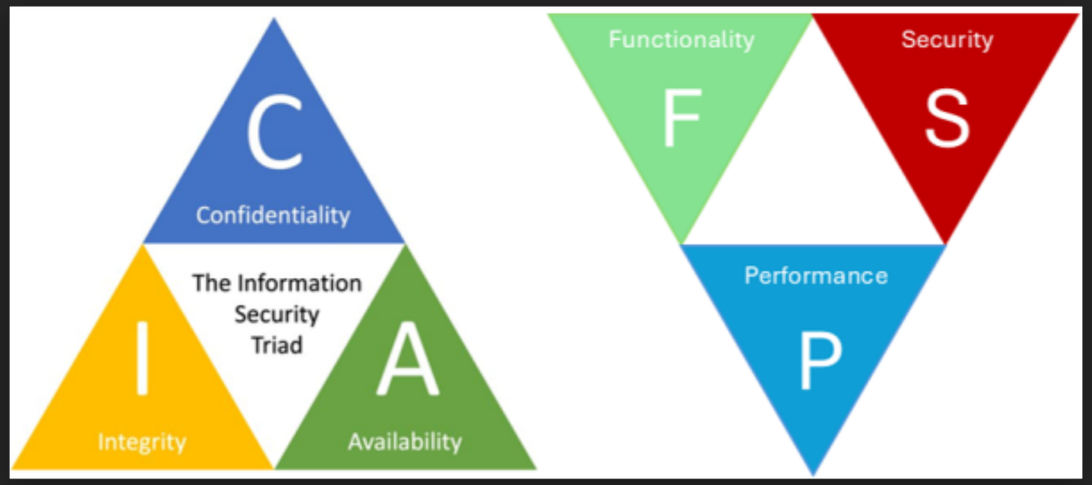
Encryption Algorithms

Algorithm	Key Type	Key Length (bits)	Strengths	Common Uses
AES	Symmetric	128, 192, 256	Fast, secure, widely used	File encryption, TLS, VPNs
DES	Symmetric	56	Weak, outdated	Legacy encryption
3DES	Symmetric	112, 168	More secure than DES but slower	Banking, legacy systems
ChaCha20	Symmetric	256	Fast, efficient for mobile/IoT	Secure messaging, mobile encryption
Blowfish	Symmetric	32-448	Flexible key sizes, strong security	File encryption, password hashing
RSA	Asymmetric	1024, 2048, 4096	Strong security, widely used	SSL/TLS, email encryption
ECDSA	Asymmetric	256, 384, 521	Efficient for digital signatures	Digital signatures, SSL/TLS
Ed25519	Asymmetric	256	Highly efficient, secure, resistant to quantum attacks	SSH, Git, digital signatures
DSA	Asymmetric	1024, 2048, 3072	Secure, used in government applications	Government applications, digital signatures
Diffie-Hellman	Asymmetric	Varies	Used for secure key exchange	Key exchange, secure communication

Asymmetric vs Symmetric: Which Should I Use?



Asymmetric vs Symmetric: Which Should I Use?



CIA Triad (Information Security)

Confidentiality (C): Ensures that sensitive information is only accessible to authorized individuals, preventing unauthorized access or disclosure.

Integrity (I): Maintains the accuracy and trustworthiness of data by preventing unauthorized modifications.

Availability (A): Guarantees that information and systems are accessible to users when needed, ensuring reliable access.

FSP Triangle (Design Trade-offs)

Functionality (F): Refers to the features and capabilities a system provides to meet user and business requirements.

Security (S): Involves protecting systems and data from threats, often requiring compromises with functionality or performance.

Performance (P): Measures how efficiently a system runs, including speed and responsiveness, which can sometimes conflict with security measures.