THE KEY CHRONICLES

THE FOSS FILES | SEASON 5 | EPISODE 2

THE CIPHER FILES

Ashutosh Birje

Pranav Gawande

Aditya Aparadh

WLUG
COMMUNITY | KNOWLEDGE | SHARE

TABLE OF CONTENT

INTRODUCTION

WLUG
COMMUNITY | KNOWLEDGE | SHARE

INTRODUCTION

WLUG
COMMUNITY | KNOWLEDGE | SHARE

ENCRYPTION - DECRYPTION

To maintain security and data integrity we need encryption and decryption technique

ENCRYPTION

Process of converting information from its original, readable form into an unreadable format

Scrambling

Plan Text

ENCRYPTION

Process of converting information from its original, readable form into an unreadable format

Scrambling

??

ENCRYPTION

Process of converting information from its original, readable form into an unreadable format

Scrambling

Cipher Text

DECRYPTION

Process of converting information into its original form, unreadable form into an readable format

Unscrambling

Cipher Text

DECRYPTION

Process of converting information into its original form, unreadable form into an readable format

Unscrambling

Plain Text

WLUG
COMMUNITY | KNOWLEDGE | SHARE

ENCODING VS ENCRYPTION

ENCODING

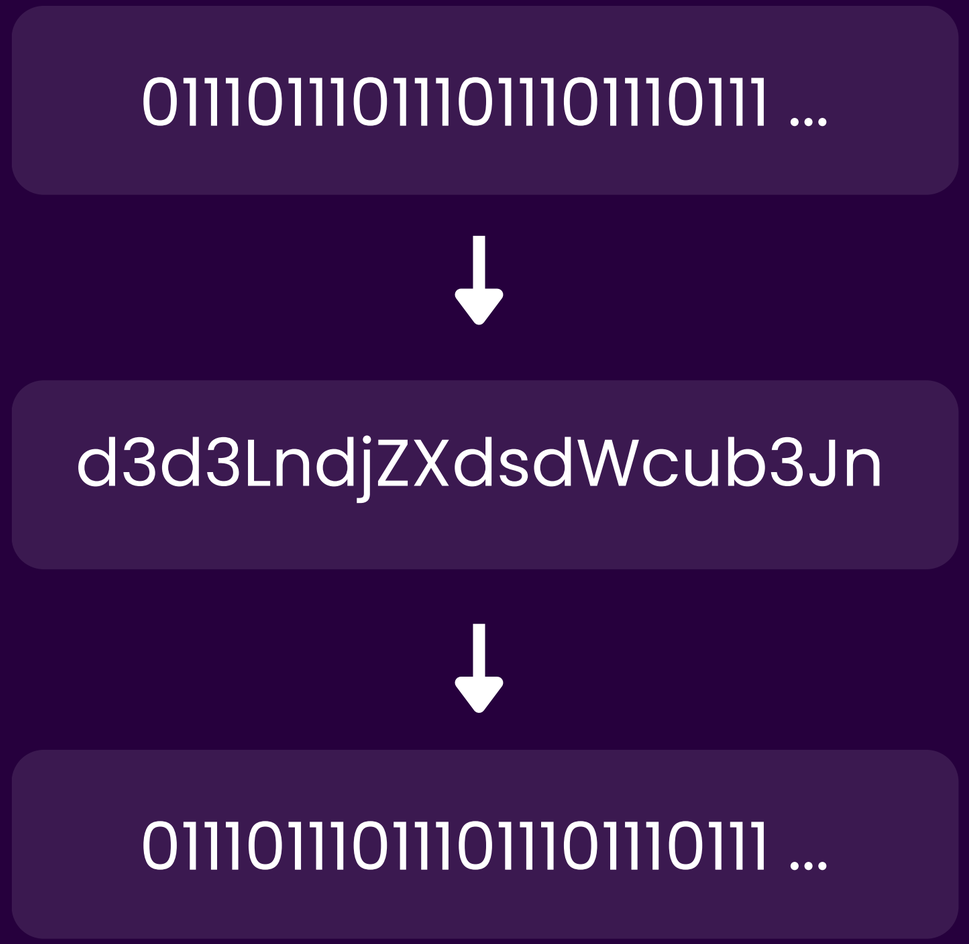
Process of converting data from one representation format to another

Can be converted back without a key

Eg- Base64, HexCode, ASCII, UTF-8

BASE64 ENCODING

- Binary to printable characters
- Useful for storing Binary data as strings, for other protocols or formats that do not support raw binary. Eg. JSON, XML
- 6 bits of binary are mapped to 1 character in the set [a-z, A-z, +,/]



ENCRPYPTION

Data

01110111011101110111011101110111 ...

00010011101110010011 ...

Key

Ciphertext

10110010011101010111001010 ...

00010011101110010011 ...

Key

Data

01110111011101110111011101110111 ...

WLUG
COMMUNITY | KNOWLEDGE | SHARE

TYPES OF ENCRYPTION

WLUG
COMMUNITY | KNOWLEDGE | SHARE

SYMMETRIC ENCRYPTION

Sachin

Ram

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Sachin

Ram

WLUG
COMMUNITY | KNOWLEDGE | SHARE

WLUG
COMMUNITY | KNOWLEDGE | SHARE

SYMMETRIC ENCRYPTION

Method of encryption where the same key is used to both encrypt and decrypt a message.

Fast and efficient

The key to be securely shared between the sender and the receiver

WLUG
COMMUNITY | KNOWLEDGE | SHARE

TYPES OF SYMMETRIC CIPHERS

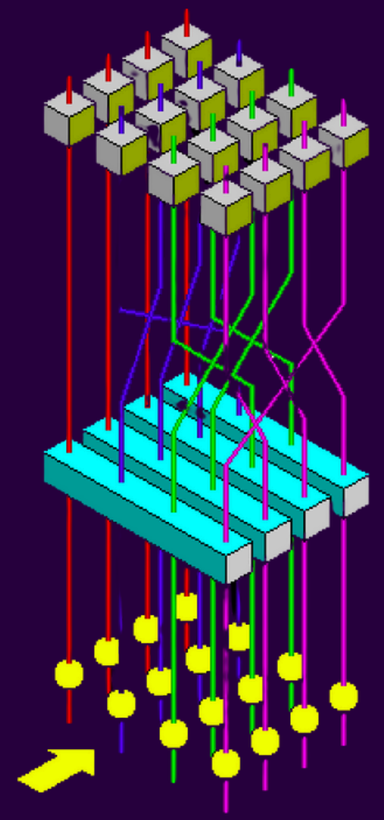
BLOCK CIPHERS

Work on fixed sized **blocks** of data

Plain text is divided into blocks, then each block is encrpyted seperately

Stateful

Considered more secure but is slower

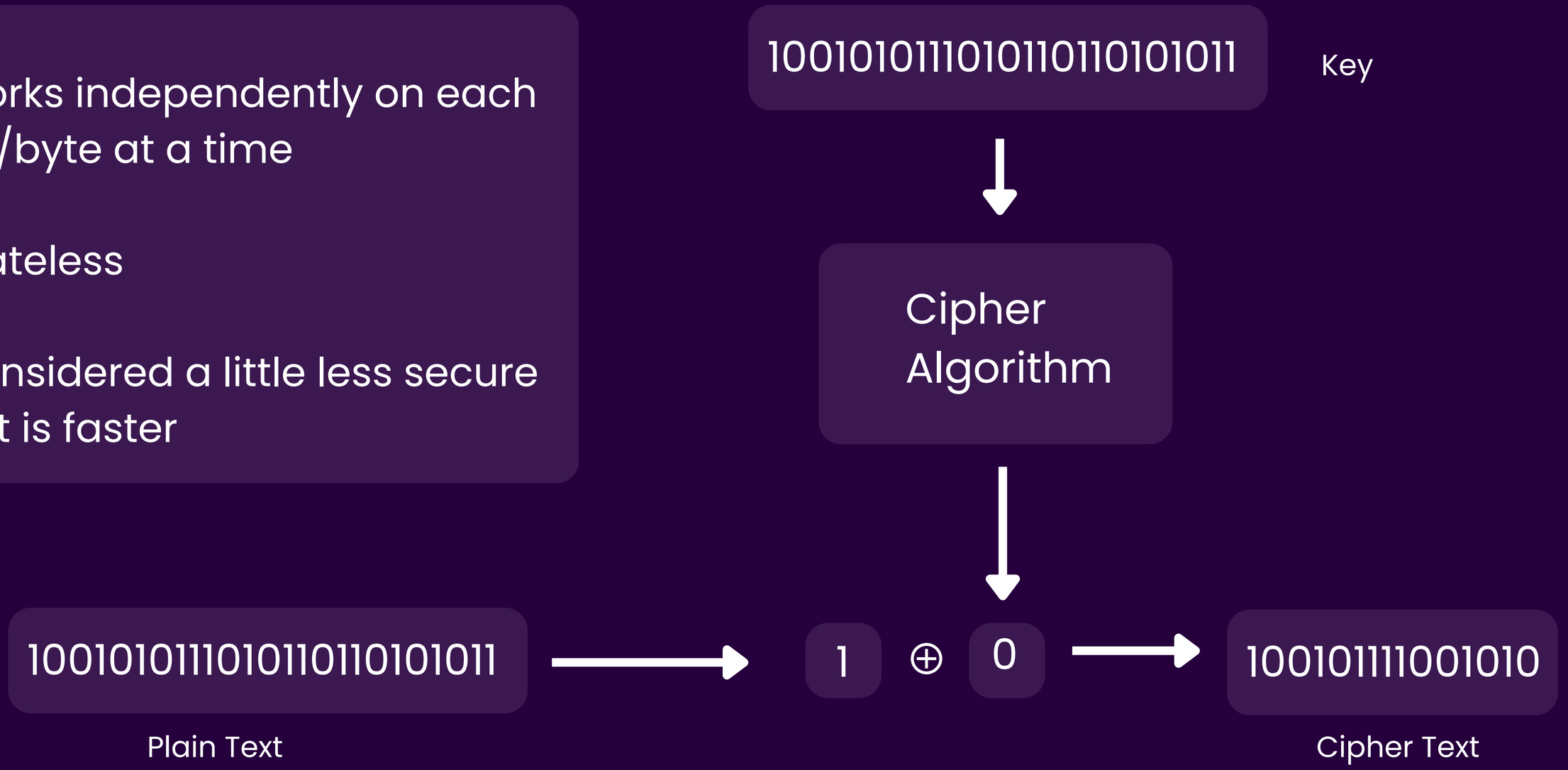


STREAM CIPHERS

Works independently on each bit/byte at a time

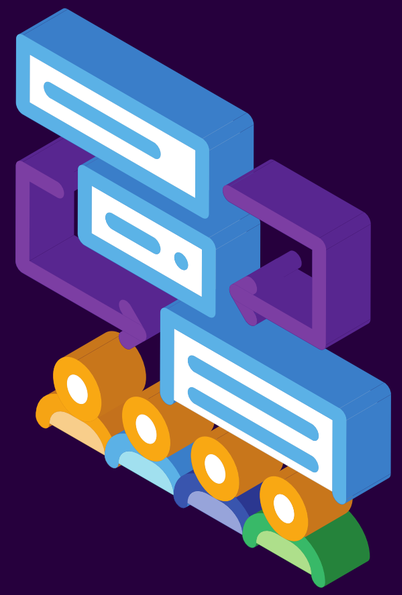
Stateless

Considered a little less secure but is faster



WLUG
COMMUNITY | KNOWLEDGE | SHARE

ALGORITHMS



WLUG
COMMUNITY | KNOWLEDGE | SHARE

List Of Algorithms

- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)
- CHACHA Cipher

DES

Encryption algorithm known for its 56 bit key length

It is based on confusion and diffusion attributes of cryptography

In the data block of 64 bit size every 8th bit of the key is discarded to produce 56 bit key

AES

Encryption algorithm known for its various key length (128, 192 , 256) bit

It performs replace and shuffle operations on bytes of data rather than in bits

Wide range of application

CHACHA

Stream cipher

Security almost on par with AES

Performs better than AES computationally

An emerging standard

WLUG
COMMUNITY | KNOWLEDGE | SHARE

ASYMMETRIC ENCRYPTION

WLUG
COMMUNITY | KNOWLEDGE | SHARE

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Issue with Symmetric Encryption

Secret key can be compromised

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Public Key

Private Key

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Maya

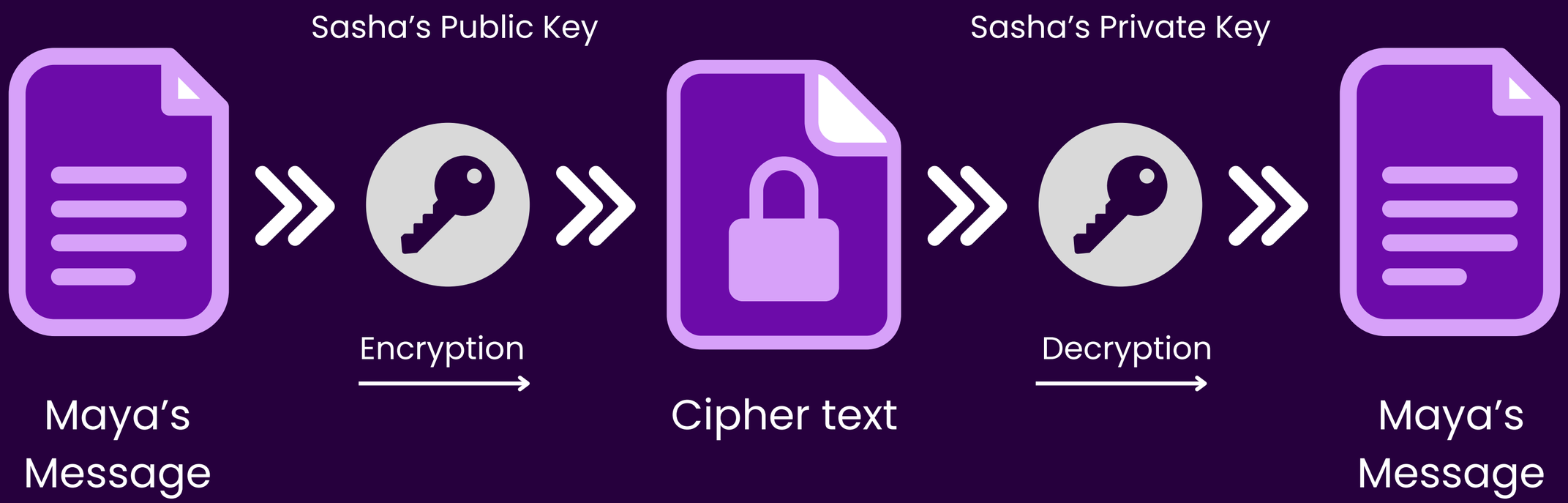
Public Key

Private Key

Sasha

Public Key

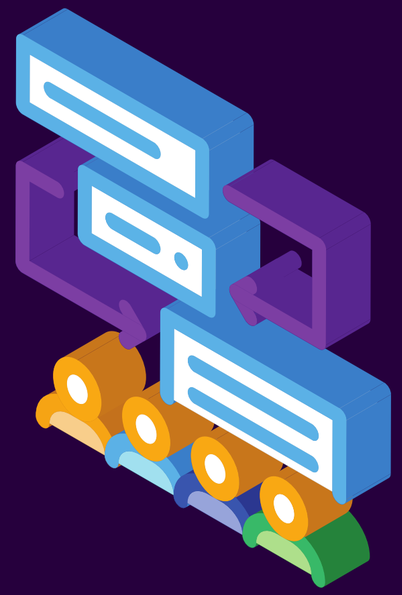
Private Key



Only public key is shared

WLUG
COMMUNITY | KNOWLEDGE | SHARE

ALGORITHMS



WLUG
COMMUNITY | KNOWLEDGE | SHARE

List Of Algorithms

- RSA (Rivest–Shamir–Adleman)
- ECC (Elliptic Curve Cryptography)
- DSA (Digital Signature Algorithm)

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Problems

- Computational Intensity
- Large Key Sizes
- Unsuitable for Large Data

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Use Cases

- **Secure Email**: Encrypting email communication
- **Digital Signatures**: Authenticating documents and software
- **SSL/TLS**: Securing websites with HTTPS
- **Key Exchange**: Safely sharing symmetric encryption keys

WLUG
COMMUNITY | KNOWLEDGE | SHARE

DIGITAL SIGNATURES

WLUG
COMMUNITY | KNOWLEDGE | SHARE

You owe me 100$

Maya

Sasha

Maya

Sasha

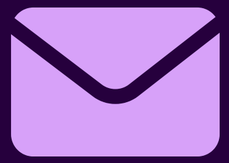
WLUG
COMMUNITY | KNOWLEDGE | SHARE

What are Digital Signatures?

- Ensures authenticity of digital data
- Uses private and public key pair
- Provides data integrity and non-repudiation
- Used in contracts, emails, transactions

Sender’s side

Maya



Maya’s text

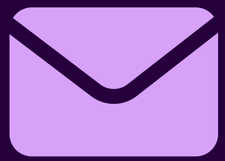
Maya’s Private Key

Digitally signed doc

Receiver’s side

Digitally signed doc

Maya’s Public Key



Maya’s text

Sasha

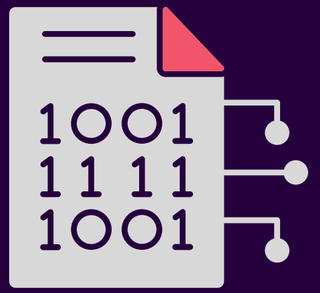
Sender’s side

Maya

Maya’s text

101001011

Hash function



Hashed message or digest

Maya’s Private Key

Digitally signed doc

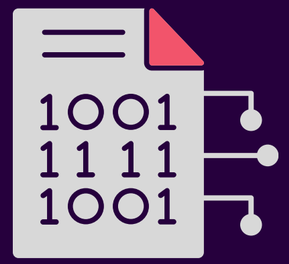
Receiver’s side

Hash function

Hashed message

Maya’s text

101001011

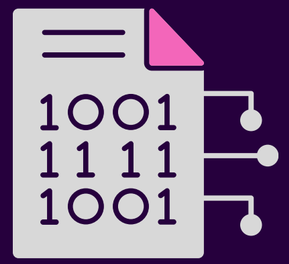


=

Sasha

Digitally signed doc

Maya’s Public Key



Decrypted hash message

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Use Cases

- Secure Email Communication
- Electronic Contracts
- Software Disribution
- Financial Transactions

WLUG
COMMUNITY | KNOWLEDGE | SHARE

SYMMETRIC Vs ASYMMETRIC

WLUG
COMMUNITY | KNOWLEDGE | SHARE

SYMMETRIC

Vs

ASYMMETRIC

Uses a single key

Uses a pair of keys

WLUG
COMMUNITY | KNOWLEDGE | SHARE

SYMMETRIC

Vs

ASYMMETRIC

SYMMETRIC		ASYMMETRIC
Uses a single key		Uses a pair of keys
Faster due to simpler algorithms		Slower due to complex computations
		

WLUG
COMMUNITY | KNOWLEDGE | SHARE

SYMMETRIC Vs ASYMMETRIC

SYMMETRIC		ASYMMETRIC
Uses a single key		Uses a pair of keys
Faster due to simpler algorithms		Slower due to complex computations
Less secure		More secure
		

WLUG
COMMUNITY | KNOWLEDGE | SHARE

SYMMETRIC Vs ASYMMETRIC

SYMMETRIC		ASYMMETRIC
Uses a single key		Uses a pair of keys
Faster due to simpler algorithms		Slower due to complex computations
Less secure		More secure
Bulk data encryption		Digital Signatures

THANK YOU