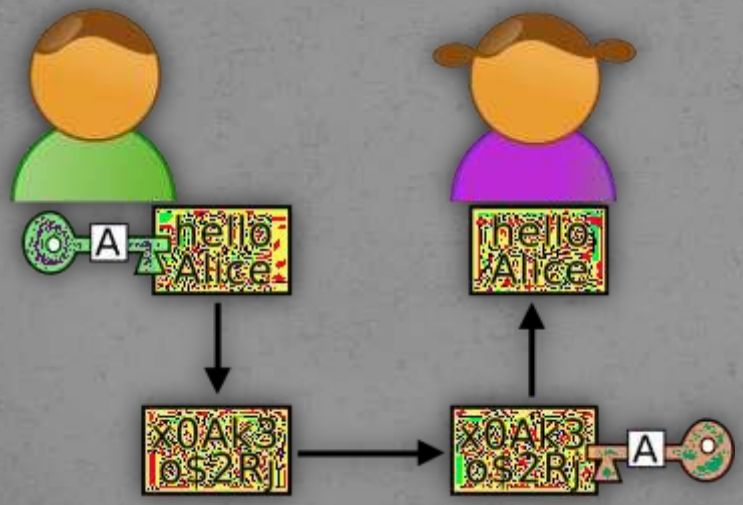
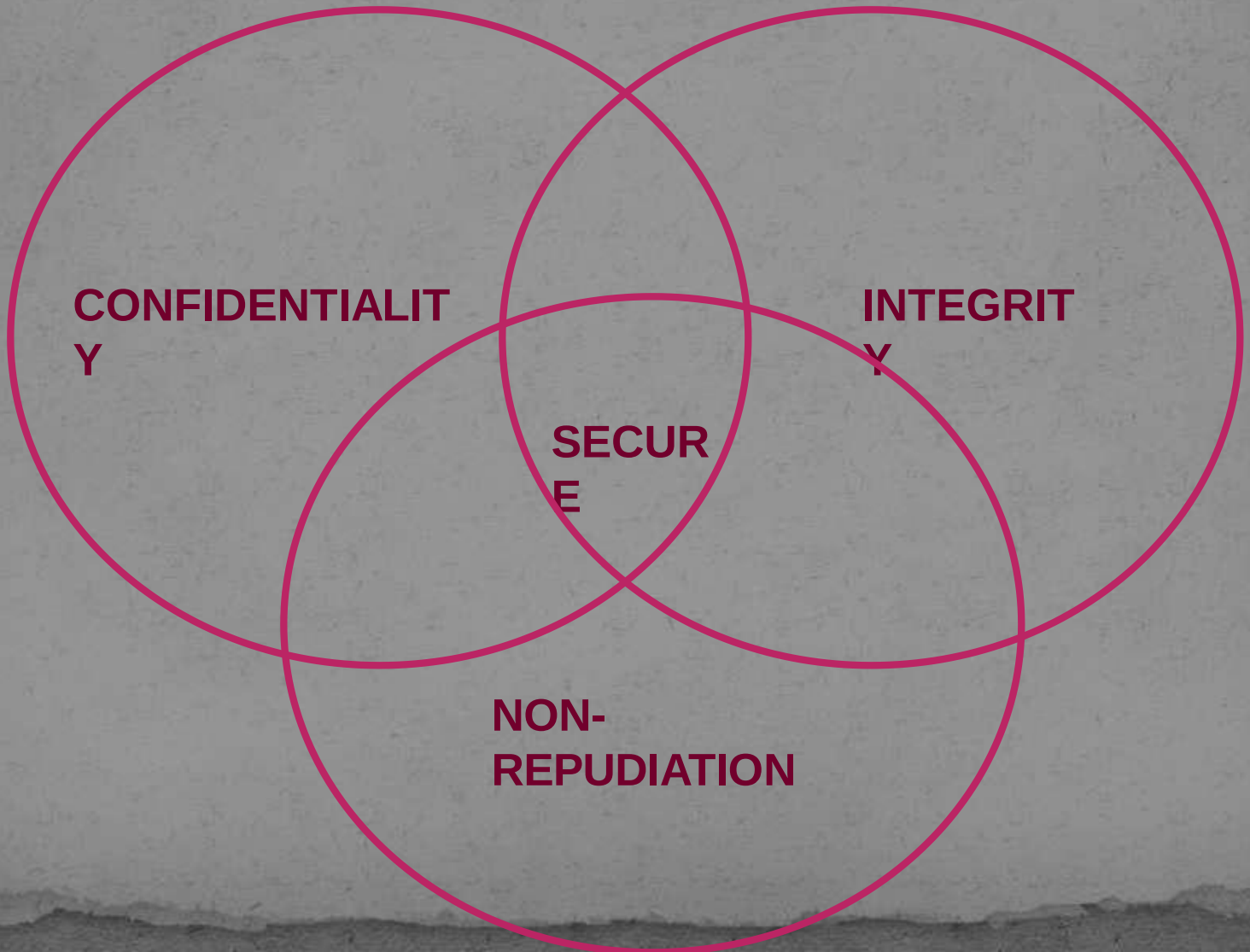
CRYPTOGRAPHY

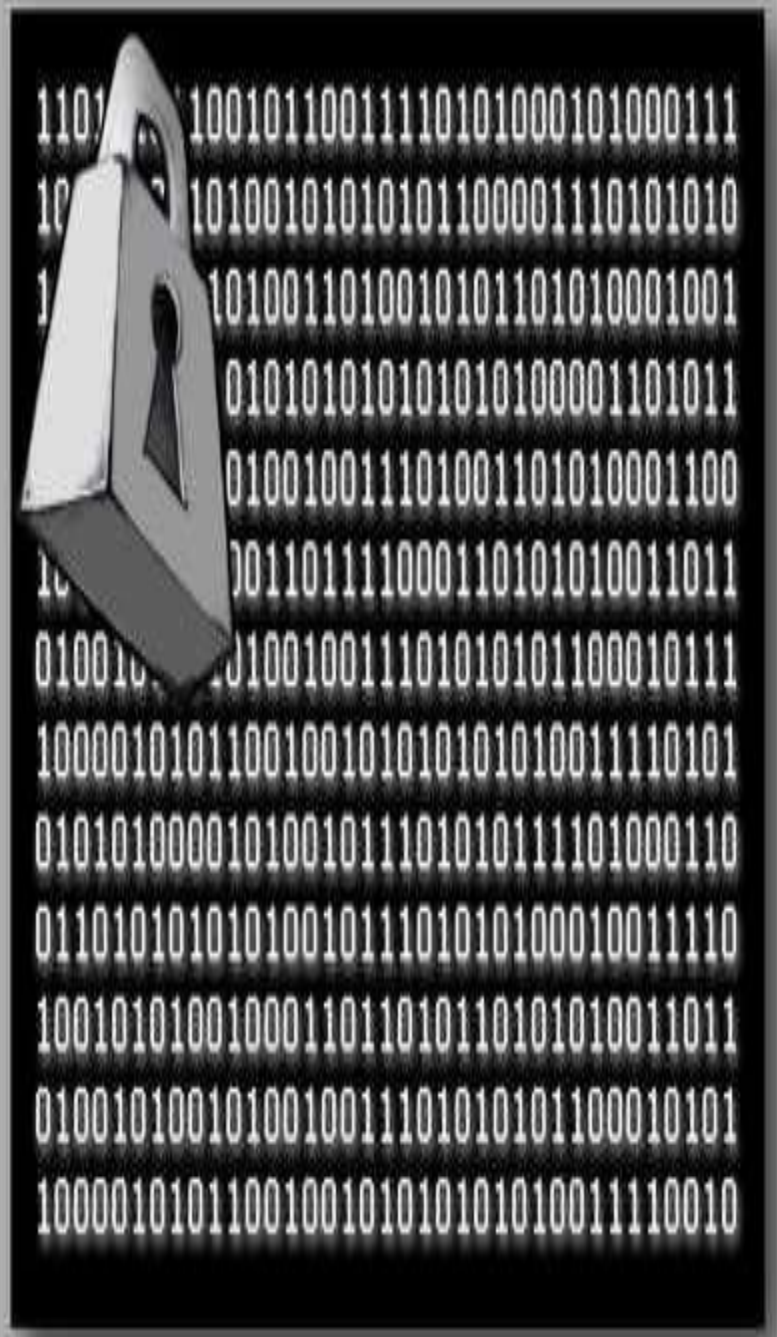


SECURITY GOALS



CRYPTOGRAPHY

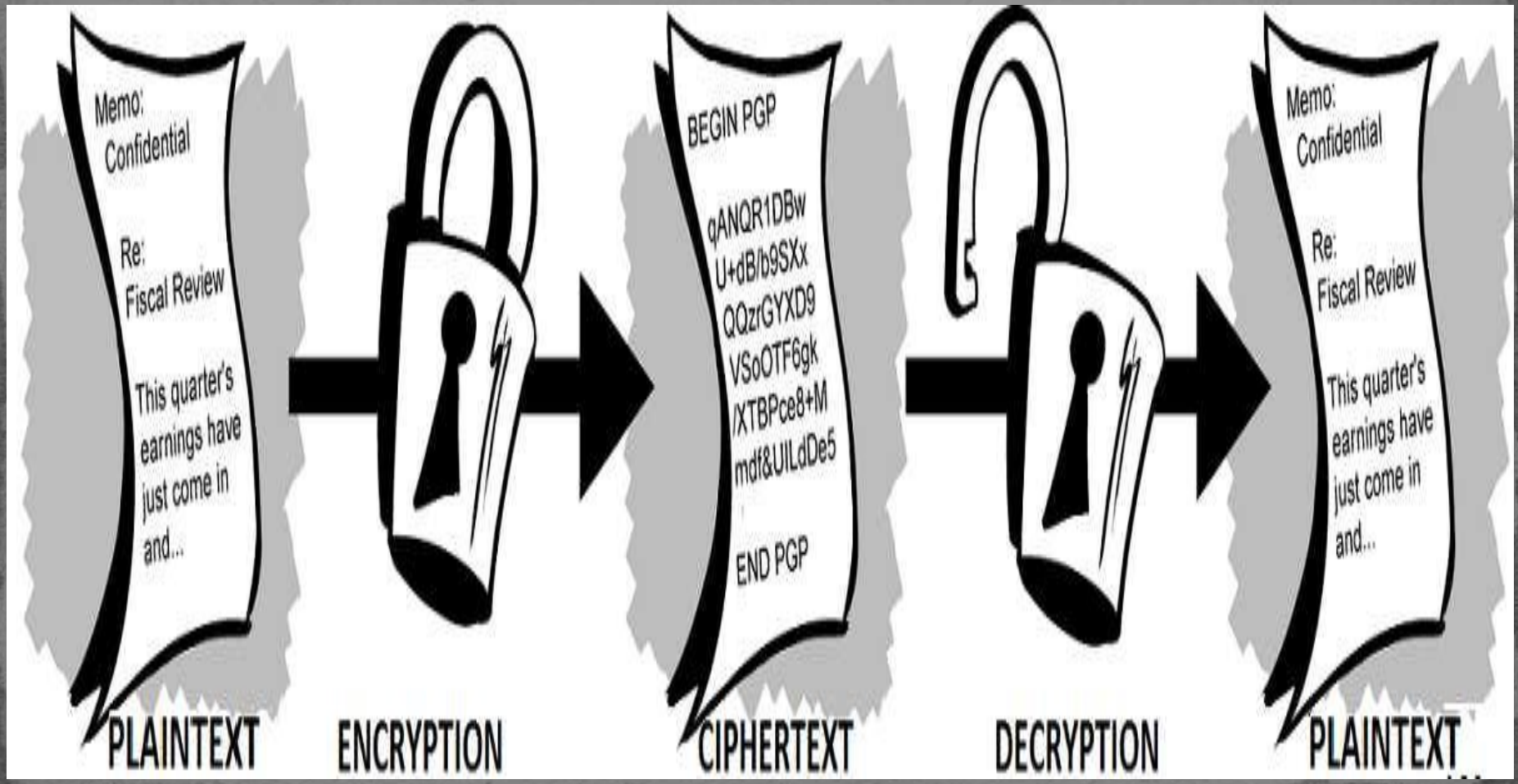
- Cryptography is the science of transforming messages to make them secure and immune to attack.



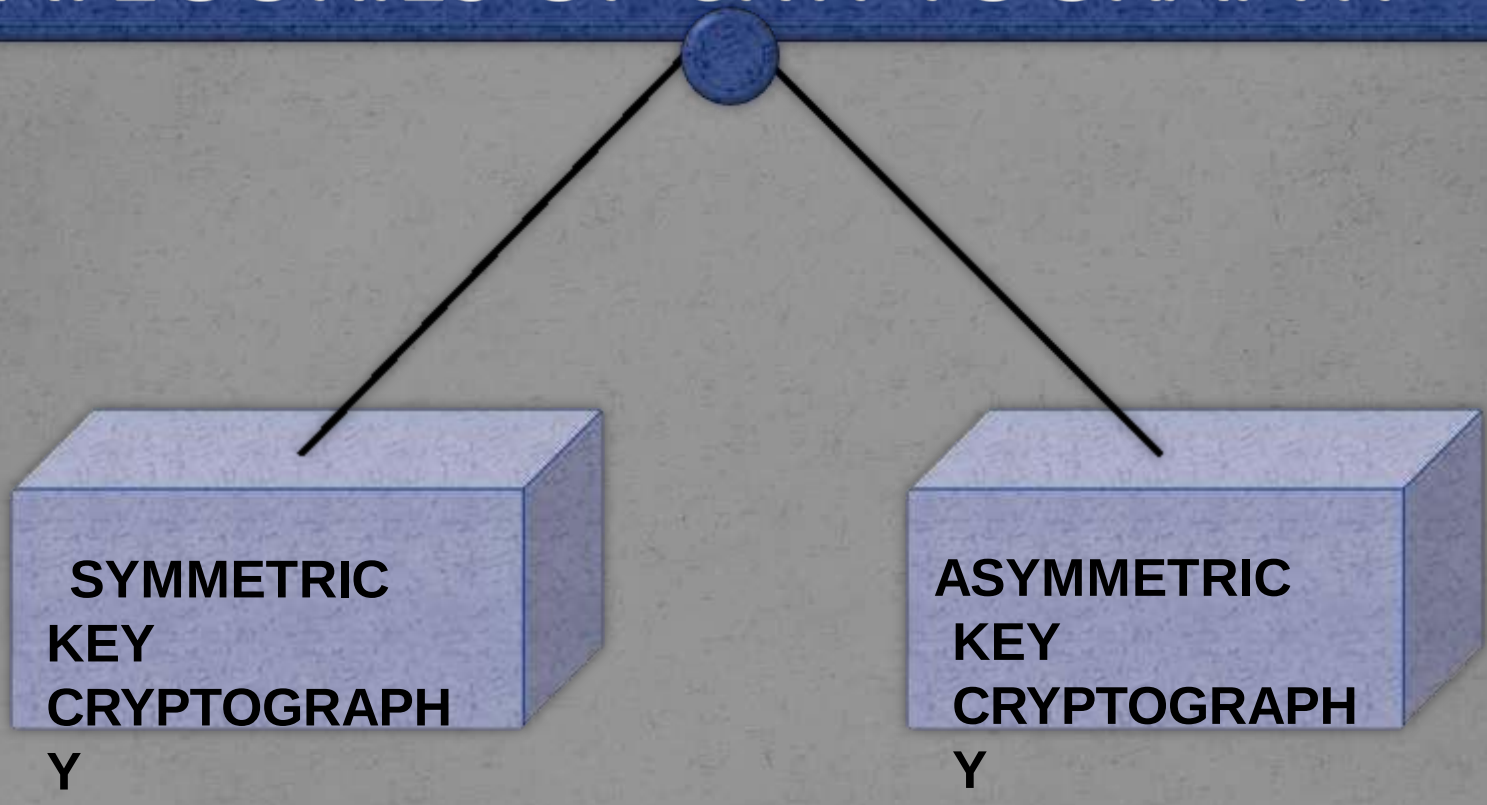
BASIC TERMS

- PLAIN TEXT
- CIPHER TEXT
- CIPHER
- ENCRYPTION & DECRYPTION
- KEYS

ENCRYPATION & DECRYPTION



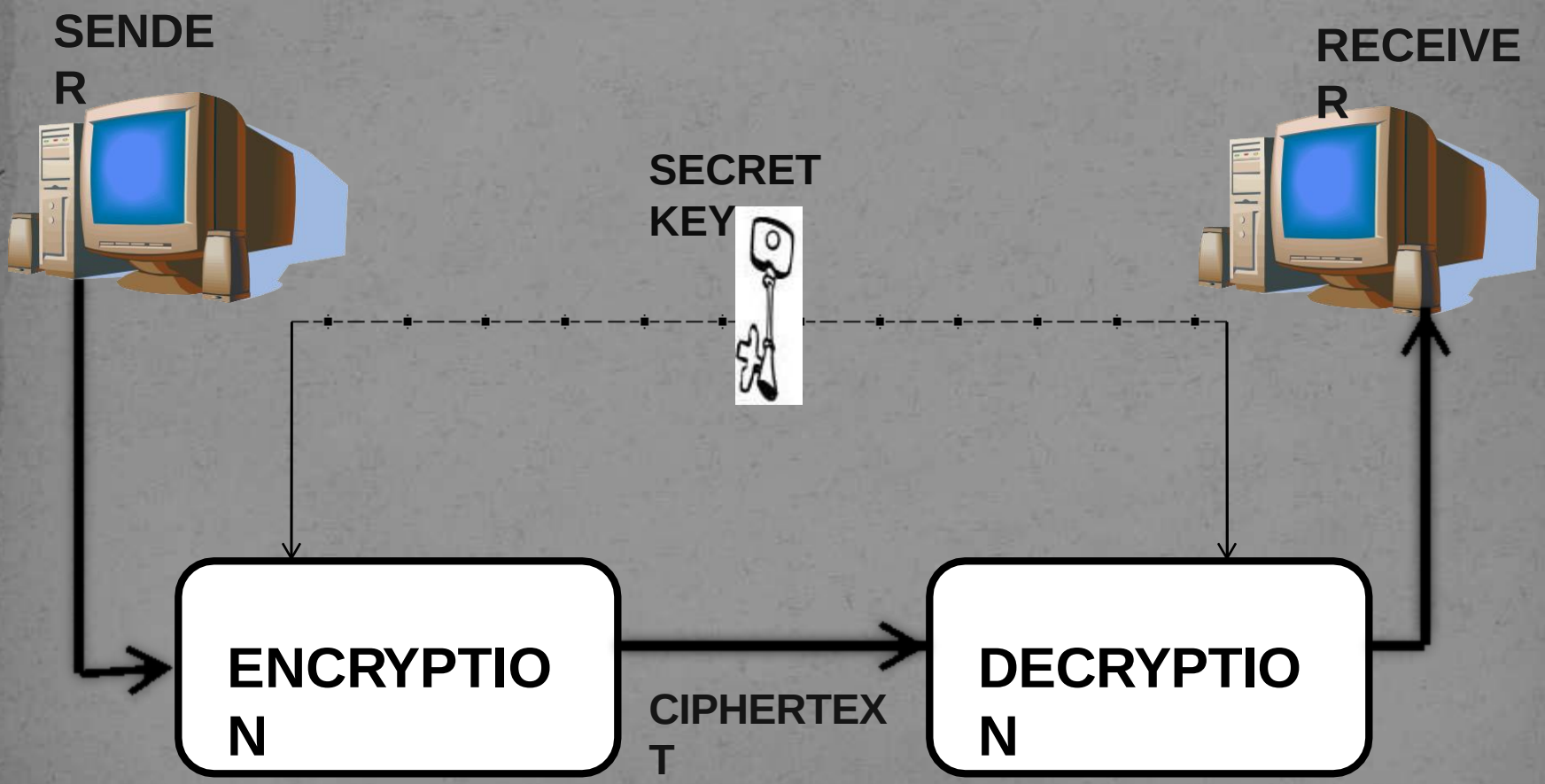
CATEGORIES OF CRYPTOGRAPHY

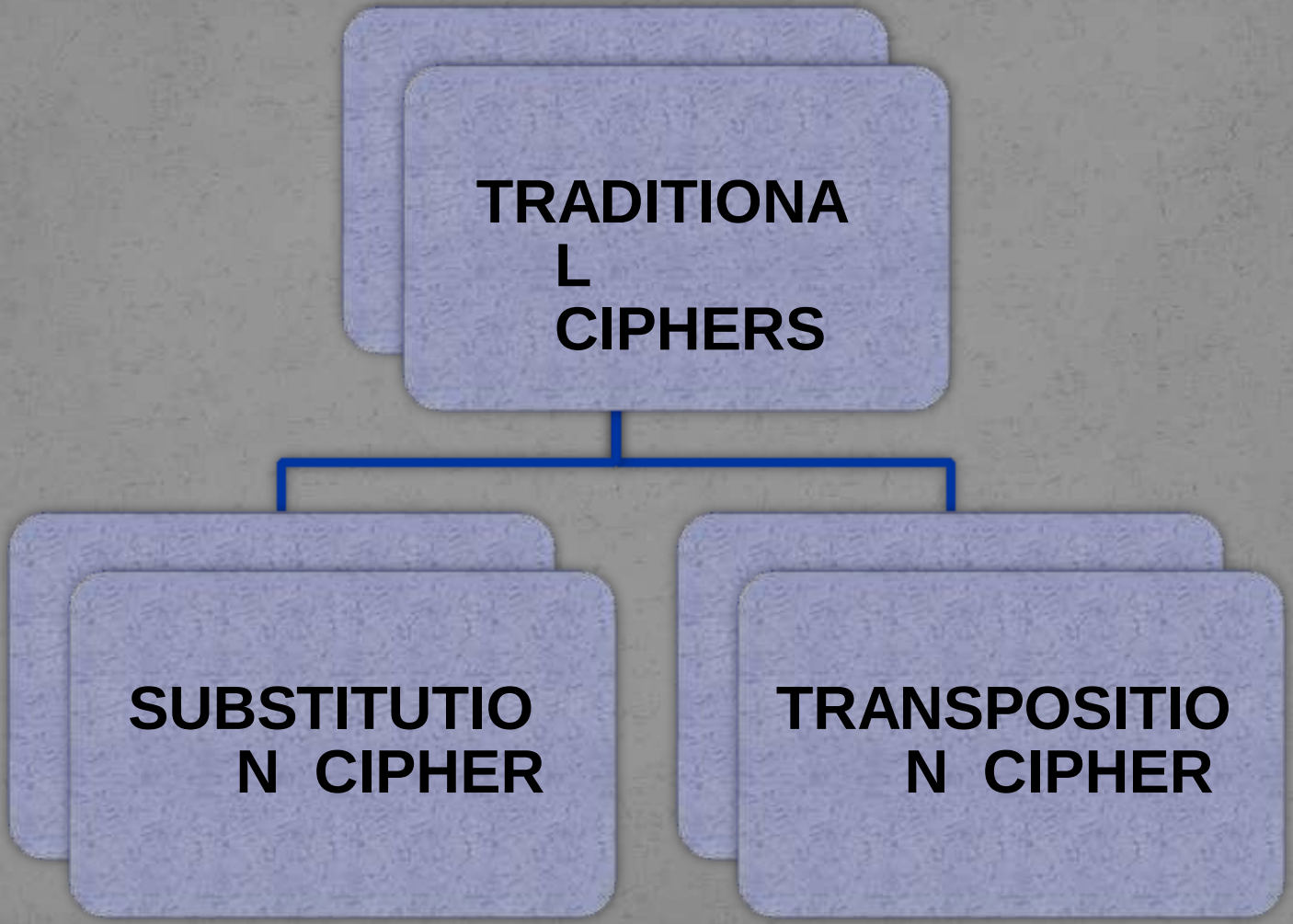


SYMMETRIC KEY CRYPTOGRAPHY

- Also known as secret key. Sender & receiver uses same key & an encryption/decryption algorithm to encrypt/decrypt data. i.e. the key is shared.

SYMMETRIC KEY CRYPTOGRAPHY




TRADITIONAL CIPHERS
SUBSTITUTION CIPHER
TRANSPOSITION CIPHER

SUBSTITUTION CIPHERS

- A substitution technique is one in which the letters/number/symbols of plaintext are replaced by other letters/numbers/symbols.

e.g. A → D, → Z

T 2 → 5, 3 → 6

TRANSPOSITION CIPHER

- In the transposition technique the positions of letters/numbers/symbols in plaintext is changed with one another.

1	2	3	4	5	6
M	E	E	T	M	E
A	F	T	E	R	P
A	R	T	Y		

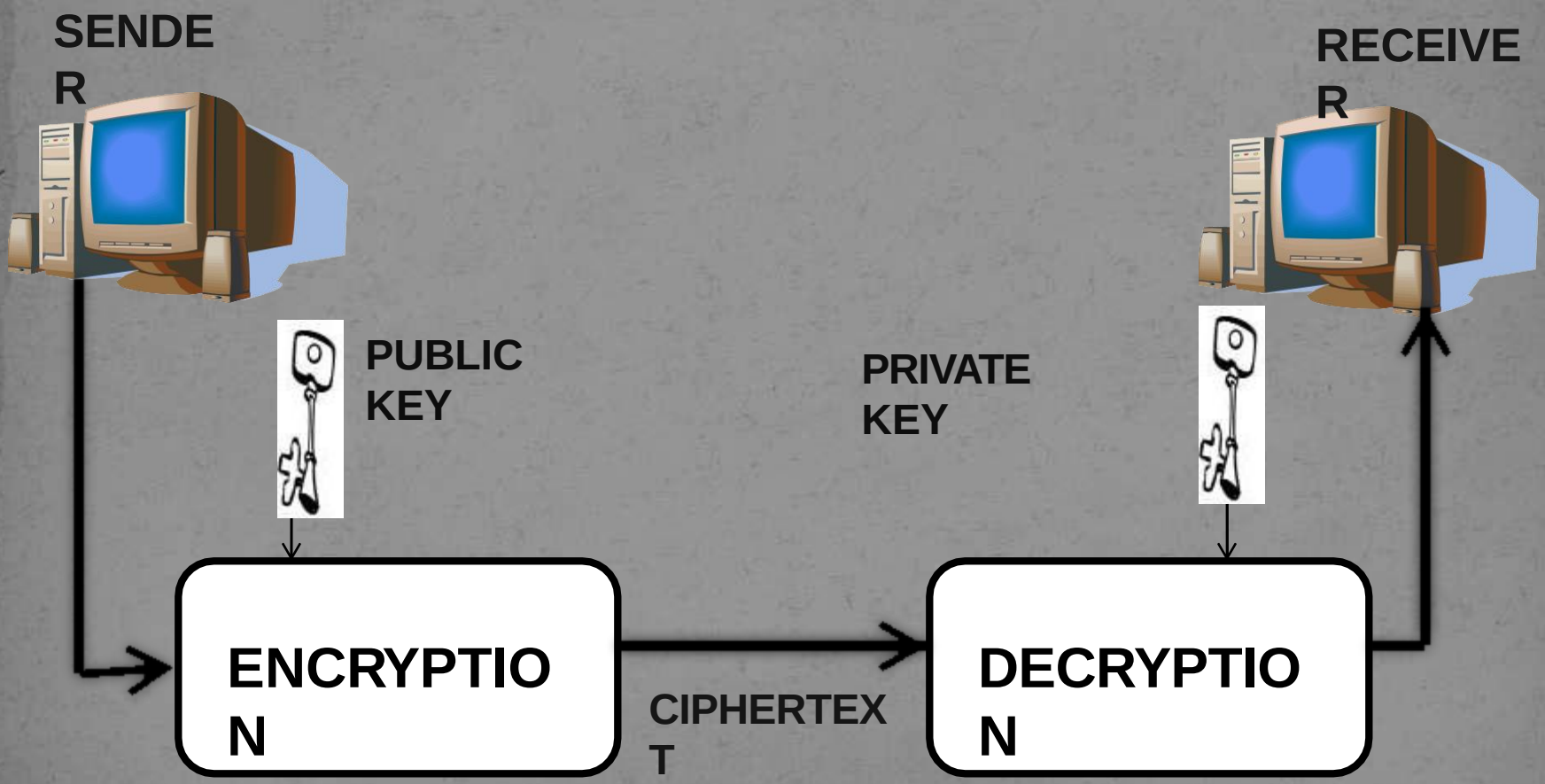
4	2	1	6	3	5
T	E	M	E	E	M
E	F	A	P	T	R
Y	R	A		T	

- Plain text: MEET ME AFTER PARTY
- Cipher text: TEMEEMEFAPTRYRAT
- KEY USED: 421635

ASYMMETRIC KEY CRYPTOGRAPHY

- Also known as public key cryptography. Sender & receiver uses different keys for encryption & decryption namely PUBLIC & PRIVATE respectively.

ASYMMETRIC KEY CRYPTOGRAPHY



KEYS USED IN CRYPTOGRAPHY

SYMMETRIC KEY CRYPTOGRAPHY

ASYMMETRIC KEY CRYPTOGRAPHY

COMPARISON

SYMMETRIC KEY CRYPTOGRAPHY	ASYMMETRIC KEY CRYPTOGRAPHY
1) The same algorithm with the same key is used for encryption and decryption. 2) The key must be kept secret. 3)It may be impossible or at least impractical to decipher a message if no other information is available.	1)One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2)One of the two keys must be kept secret. 3)It may be possible or at least practical to decipher a message if no other information is available.

DIFFERENCE BETWEEN PRIVATE (SECRET) KEY AND PUBLIC KEY

S.NO	PRIVATE KEY (SECRET KEY)	PUBLIC KEY
1	Private key is faster than public key.	It is slower than private key
2	In this, the same key (secret key) and algorithm is used to encrypt and decrypt the message.	In public key cryptography, two keys are used, one key is used for encryption and while the other is used for decryption.
3	In private key cryptography, the key is kept as a secret.	In public key cryptography, one of the two keys is kept as a secret.
4	Private key is Symmetrical because there is only one key that is called secret key.	Public key is Asymmetrical because there are two types of key: private and public key.
5	In this cryptography, the key is private.	In this cryptography, public key can be public and private key is private.

APPLICATIONS

- Defense services
- Secure data manipulation
- E –commerce
- Business transactions
- Internet payment systems
- User identification systems
- Access control
- Data security

CONCLUSION

- By using of encryption techniques a fair unit of confidentiality, authentication, integrity, access control and availability of data is maintained.

THANKS