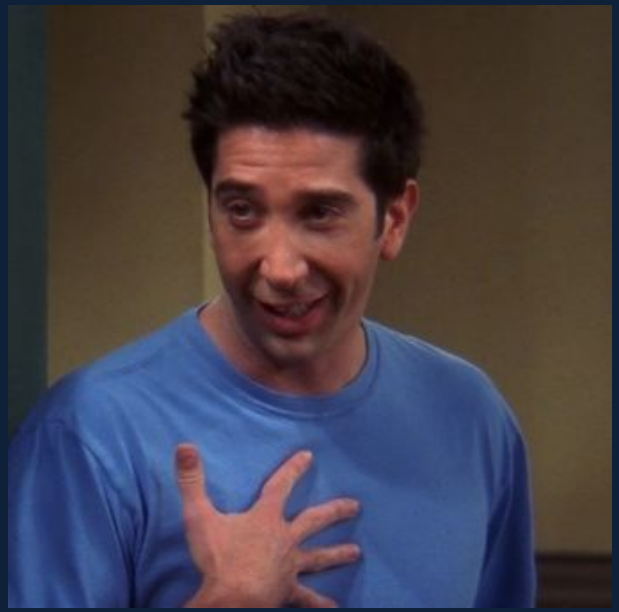
Suspicious Caesar

- When Julius Caesar sent messages to his generals, he didn't trust his messengers.
- So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the “shift by 3” rule could decipher his messages.

BASICS OF CRYPTOGRAPHY

SHUBHAM GUPTA



- 8+ Years of Experience in Security
- Mathematics Enthusiast
- Wordpress Contributor
- Part time Singer

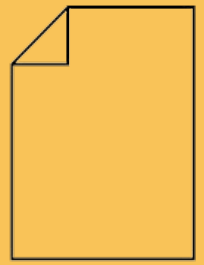
What is Cryptography?

The process and study of hiding or coding information so that only the person a message was intended for can read it

“There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files. This talk is about the later”

ENCRYPTION FRAMEWORK

Plain Text



This is an example of plain text which is not secure

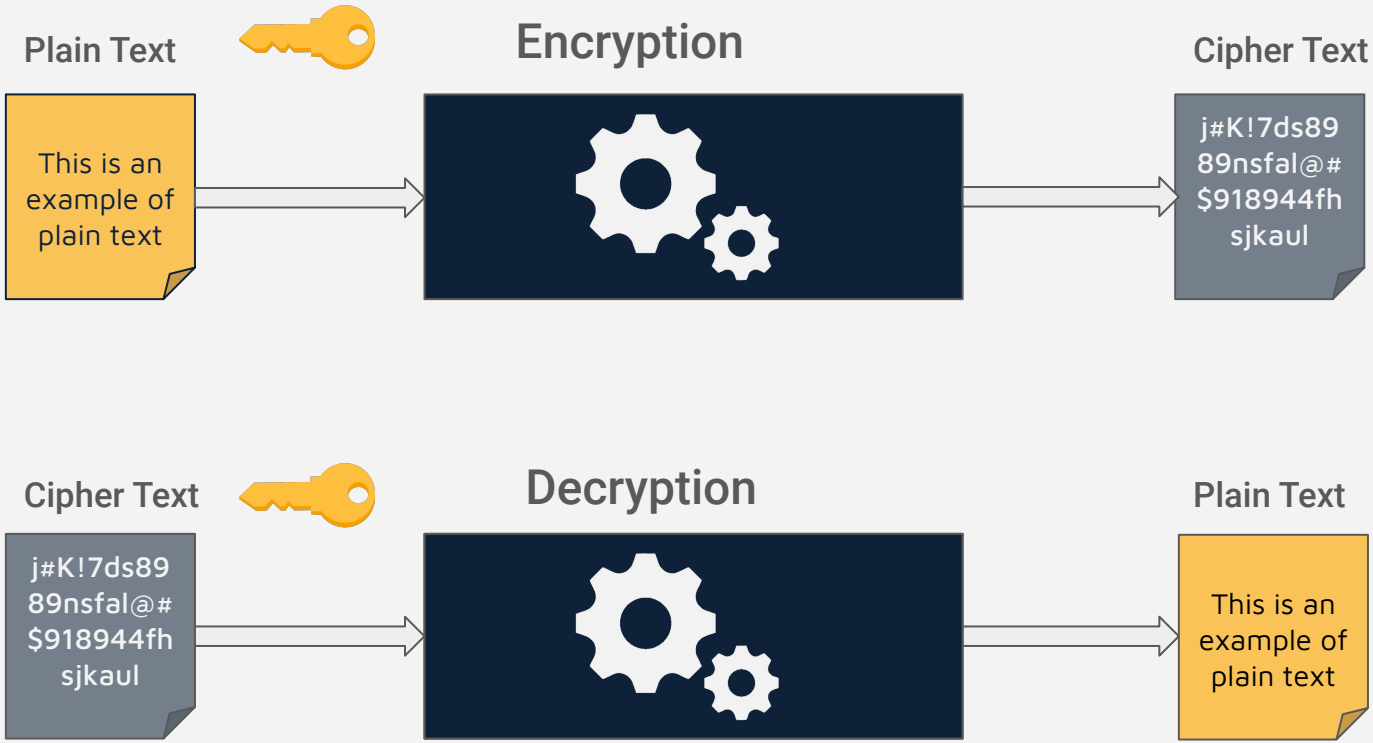
Algorithm

KEY

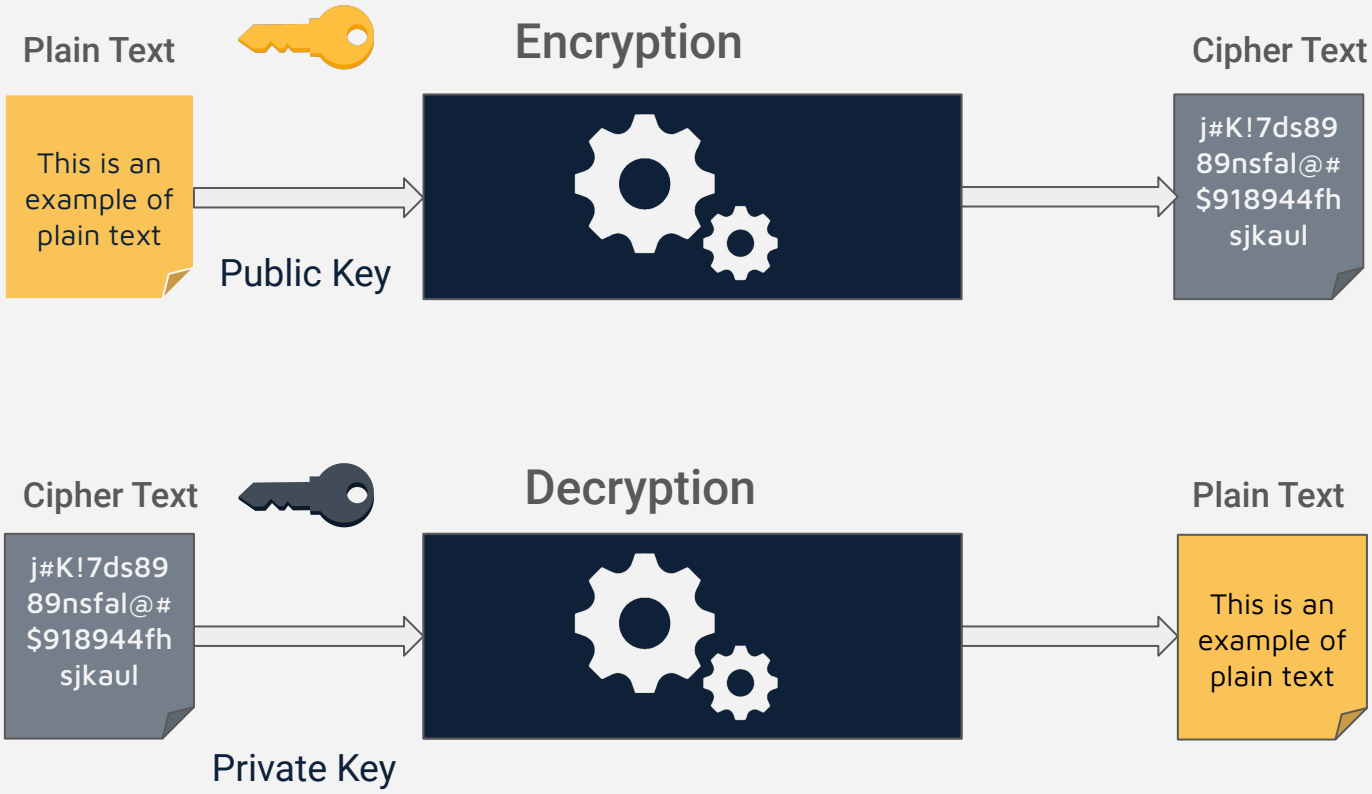
Ciphertext

j#K!7ds89
89nsfal@#$918944fhsjkaul

Symmetric Encryption



Asymmetric Encryption



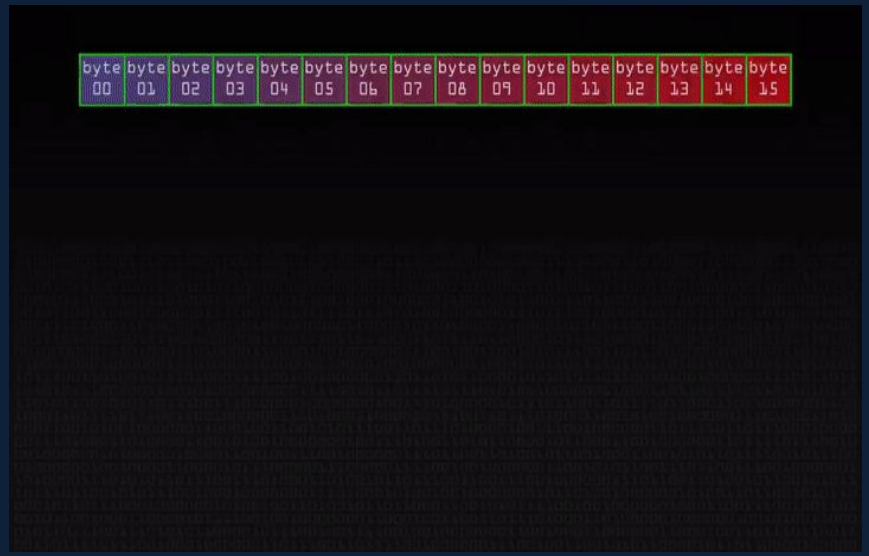
Symmetric Encryption

- Data Encryption Standard – Key Size 56 bit
- Triple DES
- Advanced Encryption Standard (AES) – Key size 128-256 bit

Asymmetric Encryption

- RSA (Rivest-Shamir-Adleman) – Key Size 1024,2048,3072,4096..
- Diffie-Hellman
- Elliptic Curve Cryptography

Understanding AES Encryption

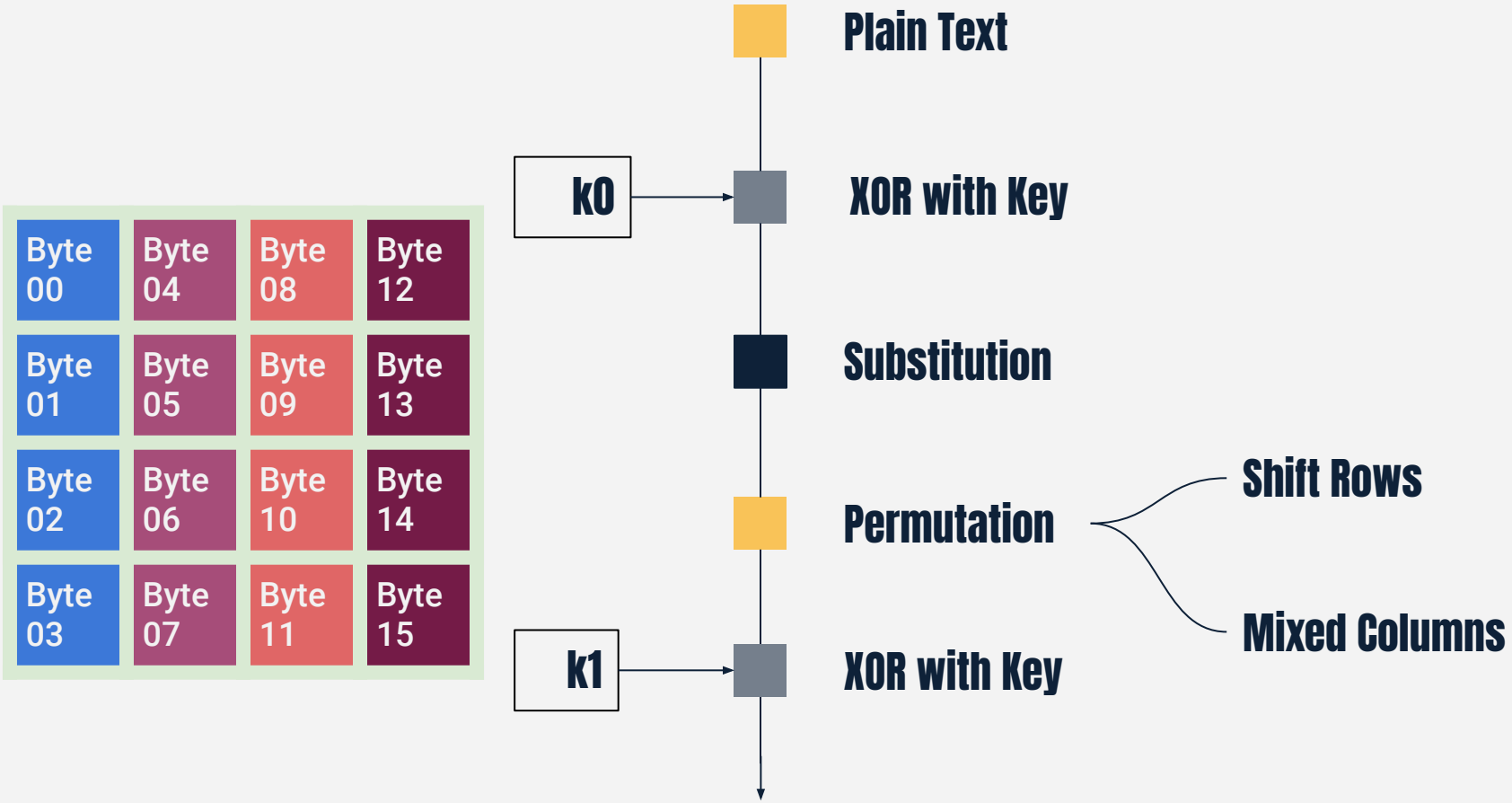


KEY SIZE

128 Bit	10 Rounds
192 Bit	12 Rounds
256 Bit	14 Rounds

* No overflowing of information

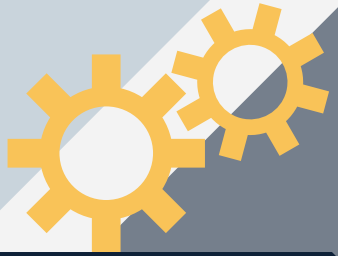
* Substitution & Permutation Networks


Byte 00
Byte 04
Byte 08
Byte 12
Byte 01
Byte 05
Byte 09
Byte 13
Byte 02
Byte 06
Byte 10
Byte 14
Byte 03
Byte 07
Byte 11
Byte 15
Plain Text
k0
XOR with Key
Substitution
Permutation
Shift Rows
Mixed Columns
k1
XOR with Key

Where is AES Encryption used?

- Wireless Security (WPA, WPA2)
- Password Managers
- Database Encryption
- AES instruction in all CPUs

PRIME & SEMI-PRIME



PRIME

Number whose factors are only 1 and itself are prime numbers like:
2,3,5,7,11,13,17..

SEMI-PRIME

Numbers whose factors are prime numbers
21 = 3 x 7
Product of prime numbers is always Semi Prime

MODULO

Remainder in a Division
13 Mod 5 = 3
21 Mode 5 = 1

Understanding RSA

Prime	P	Q	2	7
Product	N		14	
Totient	T		6	
PublicKey	E		5	
PrivateKey	D		11	

Generating Keys

- Select 2 prime numbers (P, Q)
- Calculate Product (P x Q)
- Calculate Totient (P-1)(Q-1)
- Select Public Key (E)
  - Must be Prime
  - Must be less than Totient
  - Must NOT be a factor of Totient
- Select Public Key (D)
  - Product of D and E, divided by
  - T must result in remainder 1
  - (D*E) mod T = 1

RSA Example

Prime	P	Q	2	7
Product	N		14	
Totient	T		6	
PublicKey	E		5	
PrivateKey	D		11	

Encrypt & Decrypt

Encryption: Message ^ E mod N = CipherText

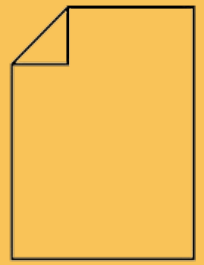
Decryption: CipherText ^ D mod N = Message

Example:

Message = B (*Let's convert it to 2*)
Cipher Text = 2 ^ 5 mod 14
= 32 mod 14 = 4 (D)
Message = 4 ^ 11 mod 14
= 4194304 mod 14 = 2 (B)

Hashing Algorithm

Plain Text



This is an example of plain text which is not secure

Algorithm

KEY

Digest

z6lf2gFu/M3EZhnyWVUH/ECPp6g=

Hash Algorithms

MD5

- Hash length 128 bit

SHA

- Hash length 128 bit

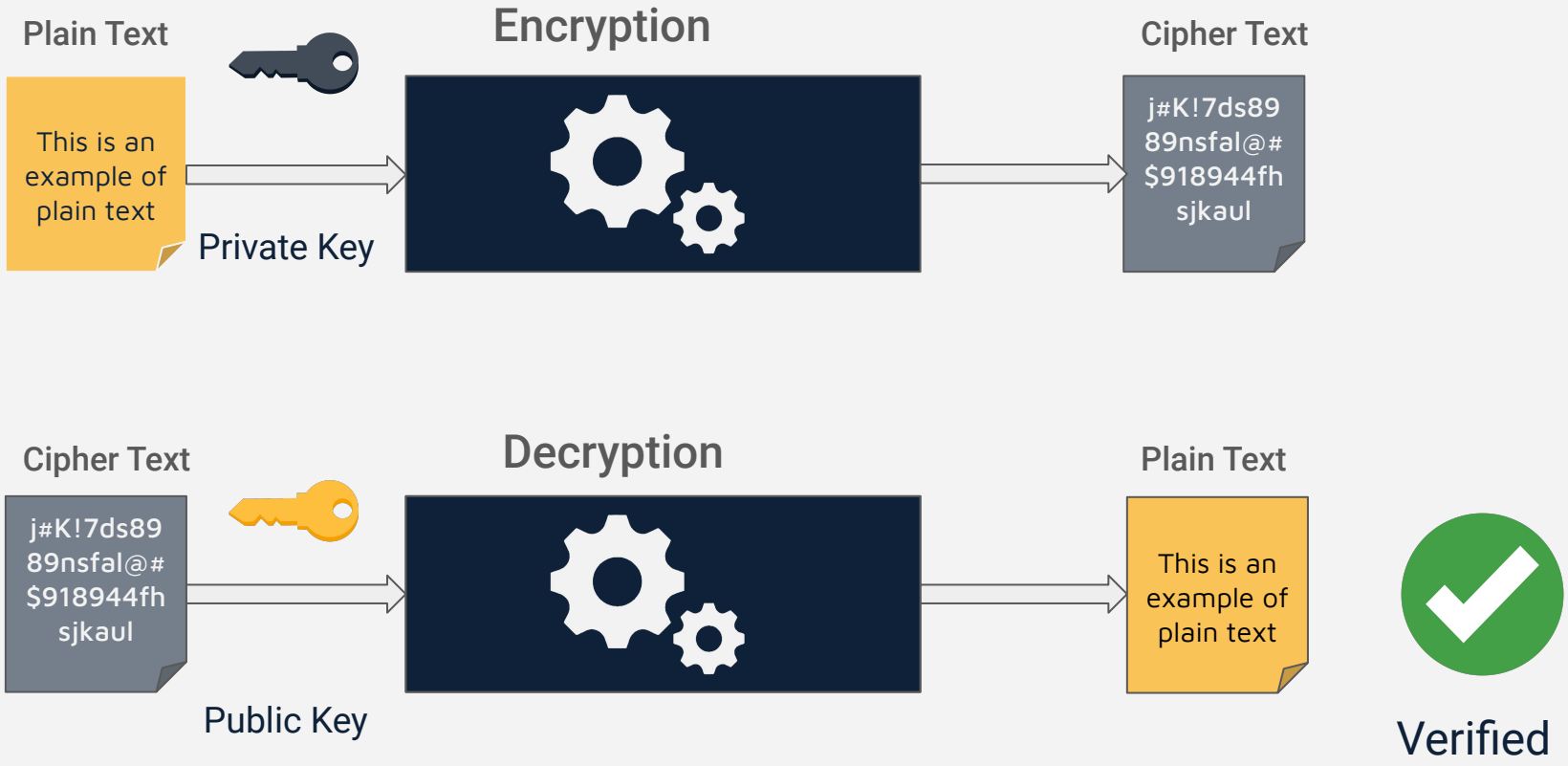
SHA - 2

- Hash length
  224
  256

RIPEMD

- Hash length
  128 bit
  160
  256
  320

Digital Signature



Takeaways

Basics of Cryptography

- What is Encryption
- Understanding types of Encryption
- Working of Advanced Standard Encryption
- Working of RSA Algorithms
- Digital Signatures

Questions ?


EUCLIDE Mathematicien
Renommé par ses Elements de Geometrie
il fleurissoit 319 avant l'ere Ch.
Cet ancien auteur, qui s'offre à tes regards
Est digne d'estre mis au rang des plus illustres
C'est luy qui rassembla ces Elements Epars
Qu'on cite même Encor, depuis quatre cent lustres

THANK YOU!