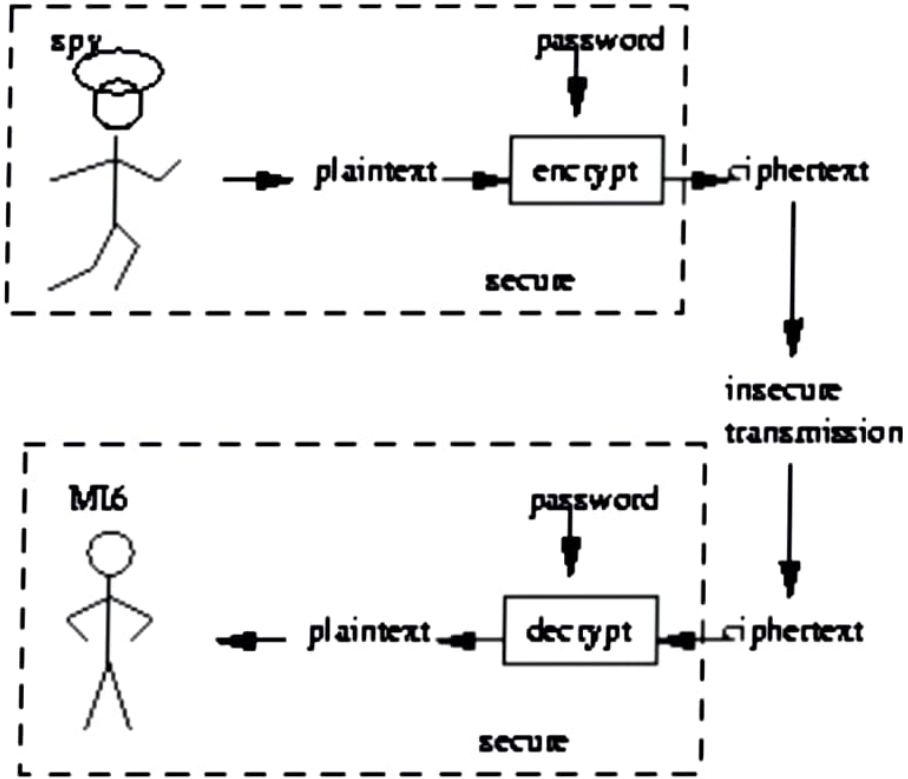
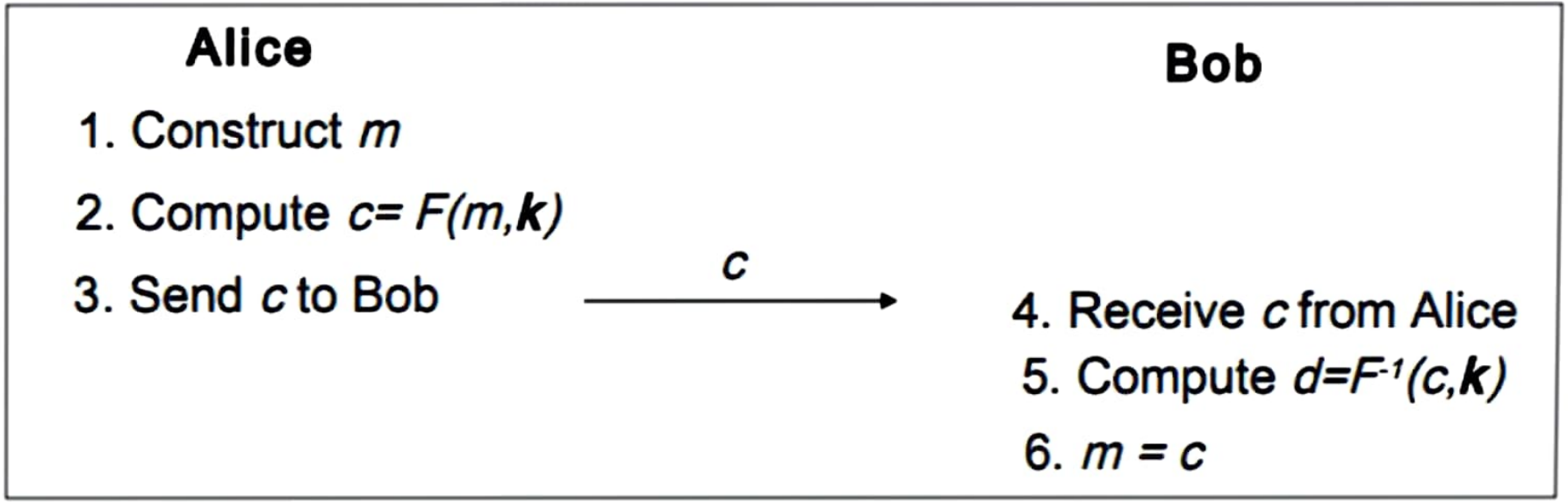
Introduction to Cryptography

Cryptography is an important aspect when we deal with network security. ‘Crypto’ means secret or hidden.



Symmetric Key Cryptography

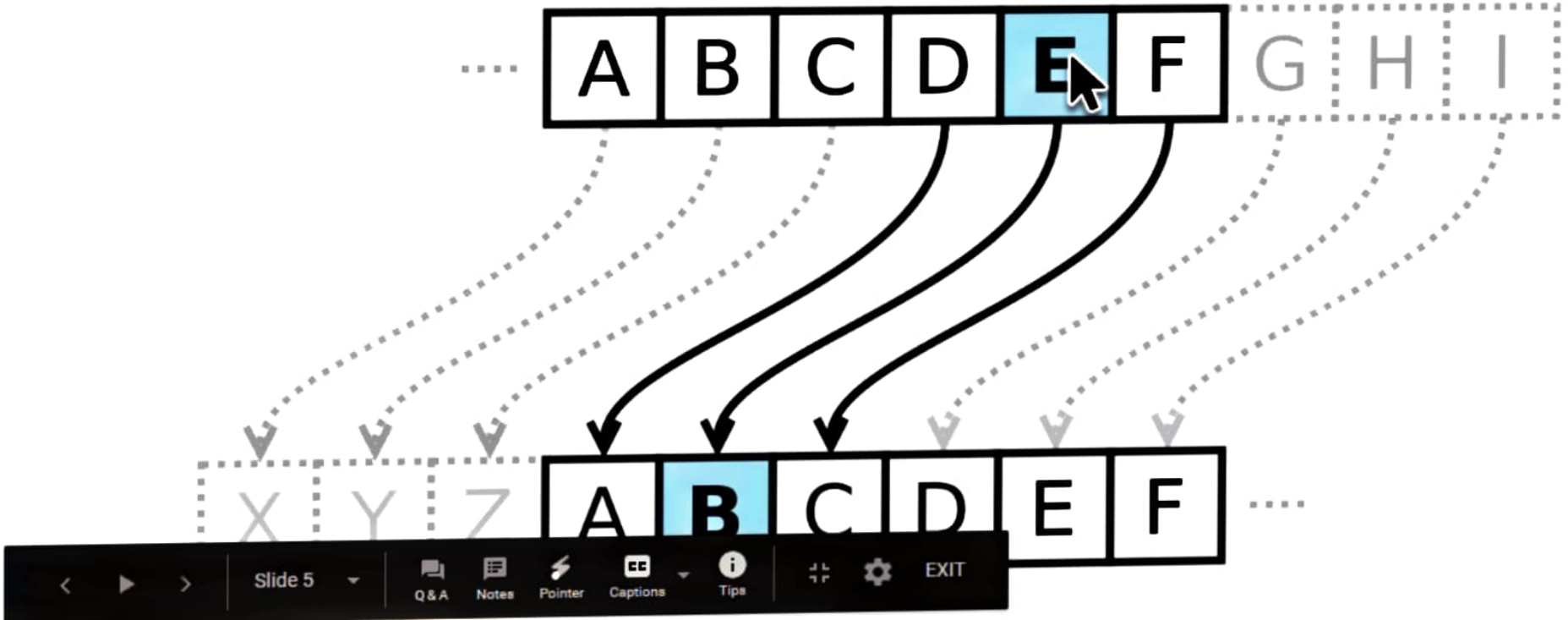
Alice encrypts a message with the same key that Bob uses to decrypt.



Eve can see c, but cannot compute m because k is only known to Alice and Bob.

Symmetric Key Cryptography

Earliest known Cryptography - Caesar Cipher



docs.google.com/presentation/d/1mhju7gWyPqxveJm4vclfSVBu_RFpTXa2NnJSbjTxatE/edit#slide=id.g82745a0a29_0_98

Introduction to Cryptography

File Edit View Insert Format Slide Arrange Tools Add-ons Help All changes saved in Drive

Present Share M

*Untitled - Notepad

File Edit Format View Help

Caesar Cipher
DES - Data Encryption Standard - 56 bit

2^

Ln 4, Col 3 100% Windows (CRLF) UTF-8

Click to add speaker notes

Explore

Symmetric Key
Symmetric Key

Alice

Message - "We are under quarantine"
Hex Message -
Symmetric Key
Encrypt(Message, Symmetric Key) - Cipher Text

Cipher Text - 176e1o87e67832tei372t923y8eyxeh9oy8do7y

Bob

Symmetric Key

1. Block Cipher - 8 bit block

Alice

Message - "We are under quarantine"

Hex Message - 7n6o3826o82368oe7736ye7o3

Bit Message - 10101010 10111111 11110000 00000001 01(

Symmetric Key - "We are still working under quarantine"

Hex Key - 38n26eo32o23y7o7yeoh7yeoyo3e39

Bit Key - 10101010 10100000 01010000 00000

Encrypt(Message, Symmetric Key) - Cipher Text

Cipher Text - 176e1o87e67832tei372t923y8eyxeh9oy8do7y

(Internet)

Bob

1. Block Cipher - 8 bit block
AES - 128 bit, 192 bit, 256 bit
Block Size - 128 bit
Key Size - 128 bit, 192, 256

Block - 128
Key = Key - Key/3 = 128

Alice

Message - "We are under quarantine"
Hex Message - 7n6o3826o82368oe7736ye7o3
Bit Message - 10101010 10111111 11110000 00000001 01(111111)

Symmetric Key - "We are still working under quarantine"
Hex Key - 38n26eo32o23y7o7yeoh7yeoyo3e39
Bit Key - 10101010 10100000 01010000 00000

Encrypt(Message, Symmetric Key) - Cipher Text

1. Block Cipher - 8 bit block
AES - 128 bit, 192 bit, 256 bit
Block Size - 128 bit
Key Size - 128 bit, 192, 256

Block - 128
Key = Key - Key/2 = 128

Alice

Message - "We are under quarantine"
Hex Message - 7n6o3826o82368oe7736ye7o3
Bit Message - 10101010 10111111 11110000 00000001 01(111111)

Symmetric Key - "We are still working under quarantine"
Hex Key - 38n26eo32o23y7o7yeoh7yeoyo3e39
Bit Key - 10101010 10100000 01010000 00000

Encrypt(Message, Symmetric Key) - Cipher Text

Stream Cipher

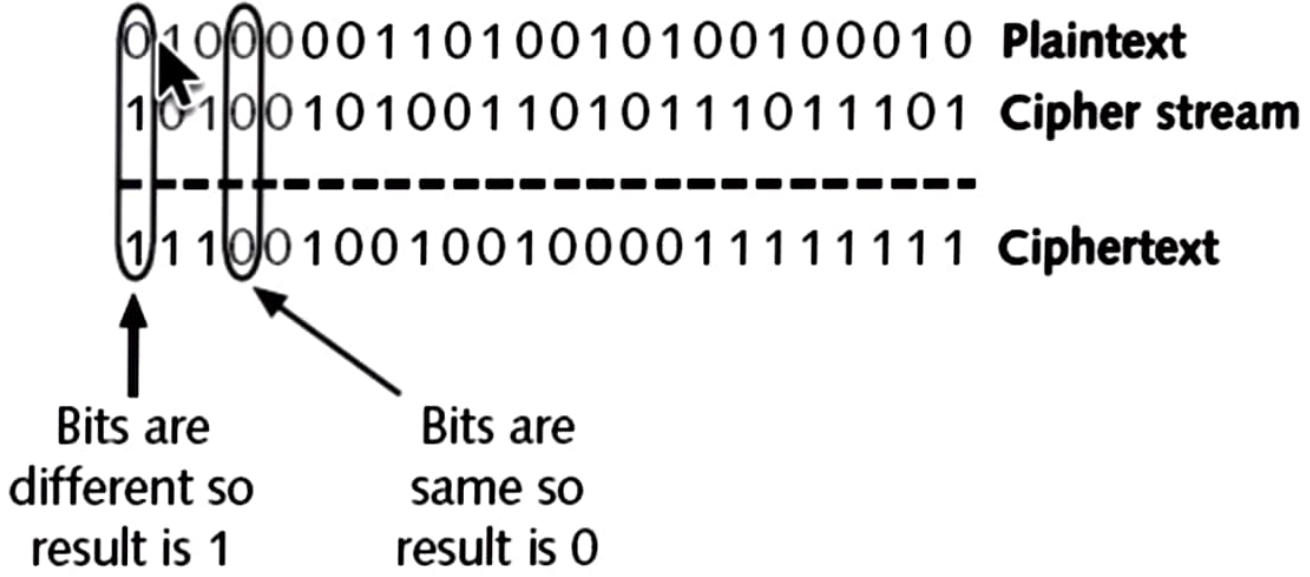
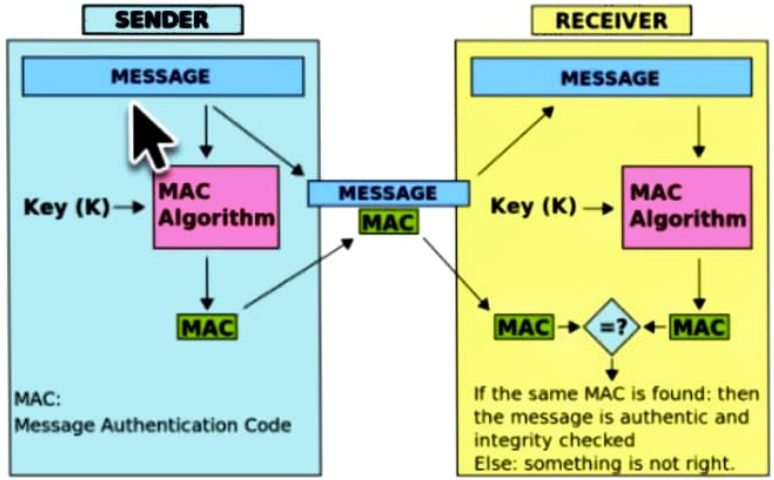


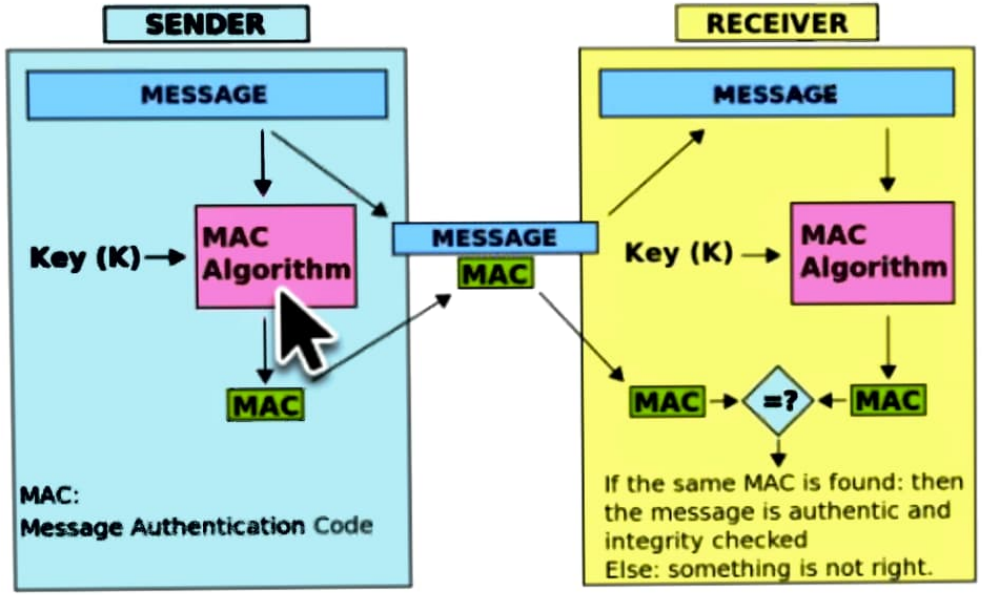
Figure 11-10 Creating ciphertext with XOR

Message Integrity



Click to add speaker notes

Message Integrity



Assymetric Cryptography
Symmetric Cryptography

Alice

Key Pair - Alice Private Key, Alice Public Key
A

Message - "Netflix has reduced the streaming to SD"

Encrypt(Message, Bob's Public Key) - Cipher Text

Cipher Text - 81yb1i7te8237t82t78o7237t832e

Bob

Cipher Text - 81yb1i7te8237t82t78o7237t832e

Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Signature hash algorithm	sha256
Issuer	GTS CA 1O1, Google Trust Ser...
Valid from	03 March 2020 15:15:25
Valid to	26 May 2020 15:15:25
Subject	*.google.com, Google LLC, Mo...
Public key	ECC (256 Bits)
Public key parameters	ECDSA_P256
Enhanced Key Usage	Server Authentication (1.3.6

```
04 e8 0a 94 b5 11 8a 57 d4 58 ad b9 f4 c1 9e
81 30 a2 27 27 71 a8 18 0f cf 4c 2c 38 5e 5a
6e 74 67 53 2c 9a ab 32 5d d0 3e 1d 4d 59 17
a7 97 98 c7 42 1b 50 b1 df 21 19 2f 40 2b 13
49 71 68 2b 24
```

Properties... | Copy to File...

OK

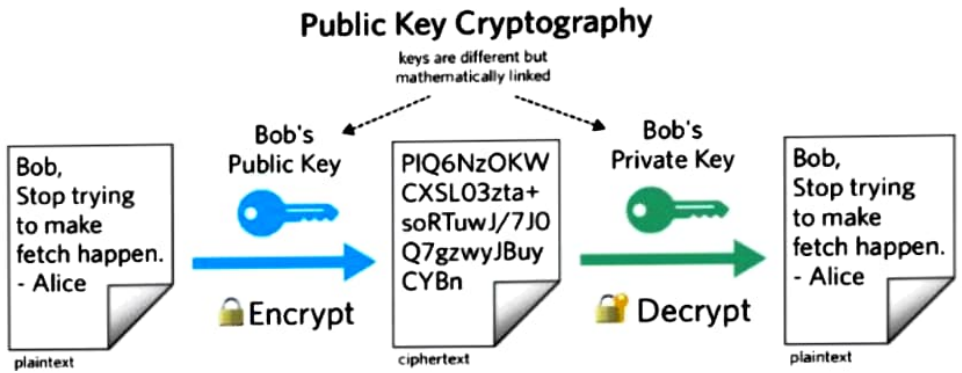
yPqxveJm4vclfSVBu_RFpTXa2NnJSbjTxatE/edit#slide=id.g82745a0a29_0_127

Tools Add-ons Help All changes saved in Drive

Present | Share | M

Background | Layout | Theme | Transition

Public Key Cryptography



10

11

Click to add speaker notes

Explore

Certification.

classfellow
DATE : / 20
PAGE No

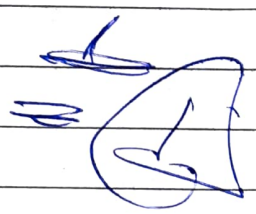
Cryptography cipher text

Plain message

DES - 56

3DES - 56*3

AES - 256



Cipher -

↳ Stream cipher - code 1 bit a time
→ Block cipher code 8 bit a time.

Symmetric Algo

AES - 128 bit, 192 bit, 256 bit.

2^{128} Brute force 2^{256}

Block size - 128 bit
Key size - 128, 192, 256

Classification of Block ciphers

MAC - Message Authentication code.

Data Integrity - | Assymetric crypto
SSL Handshake | Symetric cryptogra

Wolf SSL / Polarssl / OpenSSL

classfellow
DATE : / 20
PAGE No

IS this MAC IS Similar to What we ~~see~~ Know as MAC Address.

SHA256
~~SHA~~ | Tera byte transfered – 256 recived
What to do with data loss.

3
~~7~~.47%
2
55
65
~~50~~ 37.35
6

37.35
6
5