

4CS401

Cryptography and Network Security

By,

Manik K. Chavan

Assistant Professor, CSE Department

Walchand College Of Engineering, Sangli.

manik.chavan@walchandsangli.ac.in

Mob. 7507760777/9545413443

Prerequisite

Computer Networks

Mathematical background

Syllabus

Module-I: INTRODUCTION

Module-II: SYMMETRIC KEY CRYPTOGRAPHY

Module-III: PUBLIC KEY CRYPTOGRAPHY

Module-IV: MESSAGE AUTHENTICATION AND INTEGRITY

Module-V: NETWORK SECURITY

Module-VI: SYSTEM SECURITY

Course Learning Outcomes



CO1: apply different encryption and decryption techniques to solve problems related to confidentiality and authentication.



CO2: Analyze and apply system security concept to recognize malicious code.



CO3: analyze different attacks on networks and evaluate the performance of firewalls and security protocols like SSL, IPSec, and PGP



CO4: Apply the knowledge of cryptographic checksums and evaluate the performance of different message digest algorithms for verifying the integrity of varying message sizes.

Agenda



Why Cryptography and Network Security?



What is Cryptography



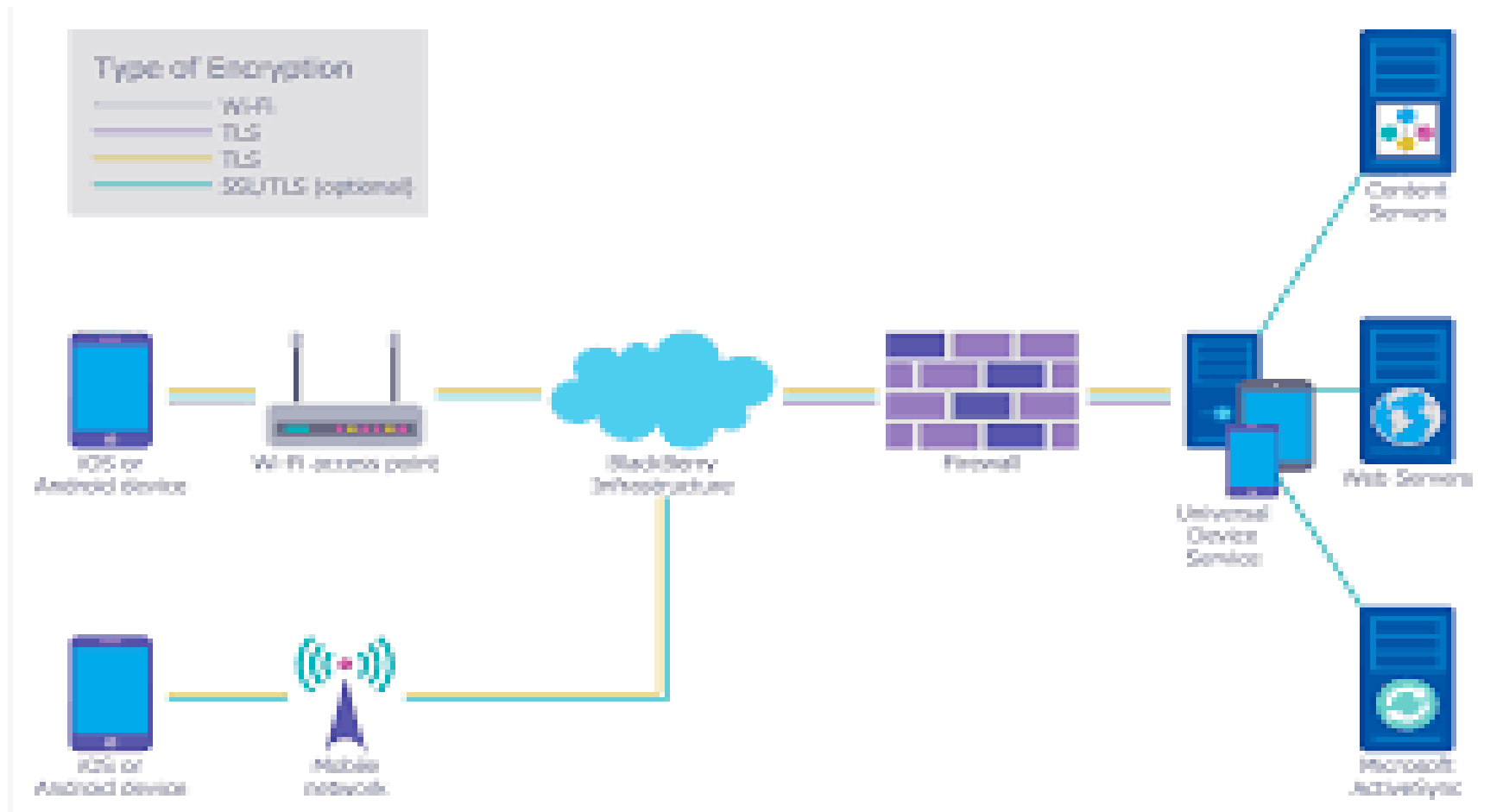
Classification of cryptography



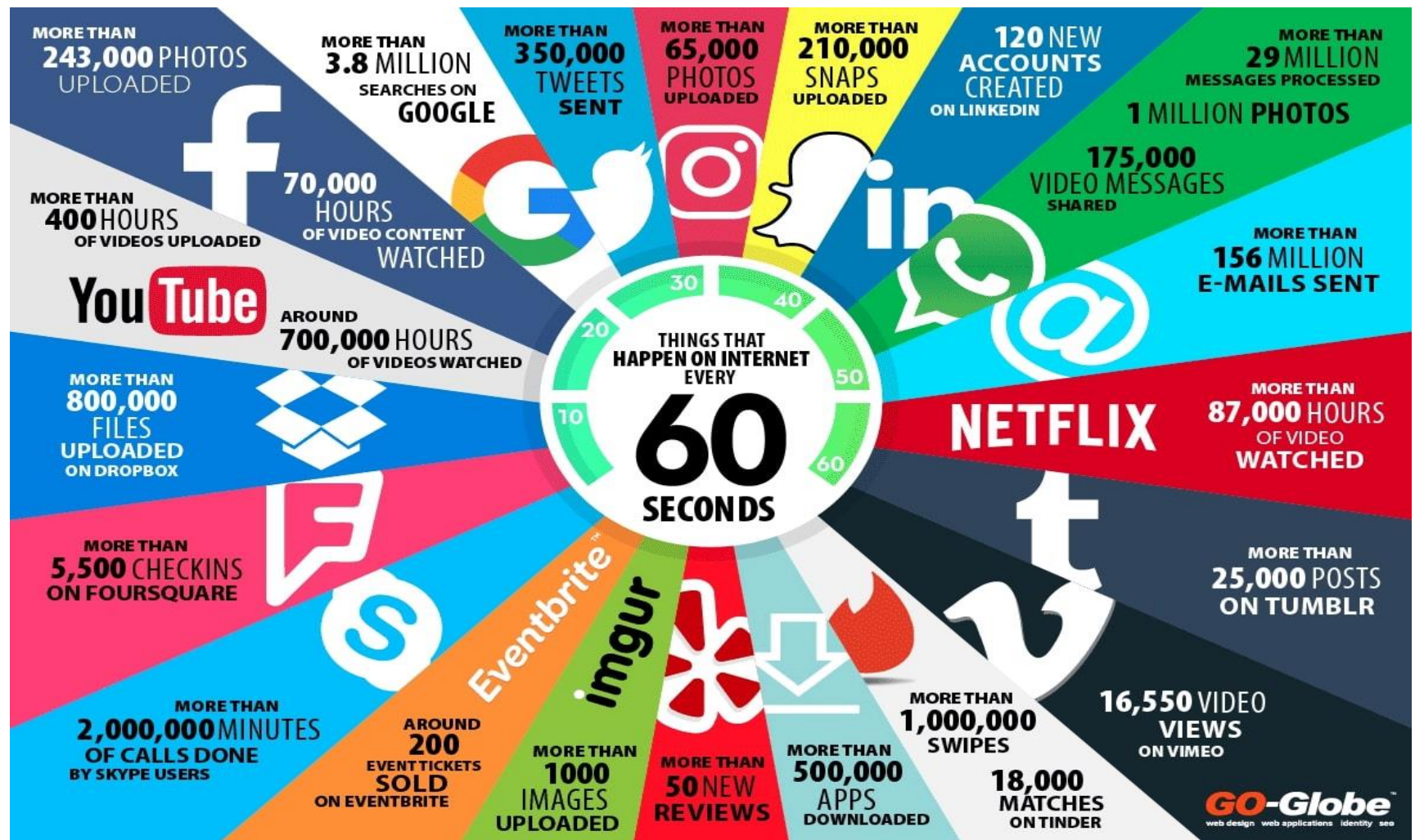
How various cryptographic algorithm works



Need for Network Security



Internet statistics-2020!



Increased Security Breaches



On March 21, 2019, **FACEBOOK** admitted that since 2012 it has not properly secured the passwords of as many as **600 MILLION USERS**.

IdentityForce

VARONIS

There was an **80% INCREASE** in the number of people affected by **HEALTH DATA BREACHES** from 2017 to 2019.

Statista



VARONIS

YAHOO holds the record for the largest data breach of all time with **3 BILLION COMPROMISED ACCOUNTS**.

Statista



VARONIS

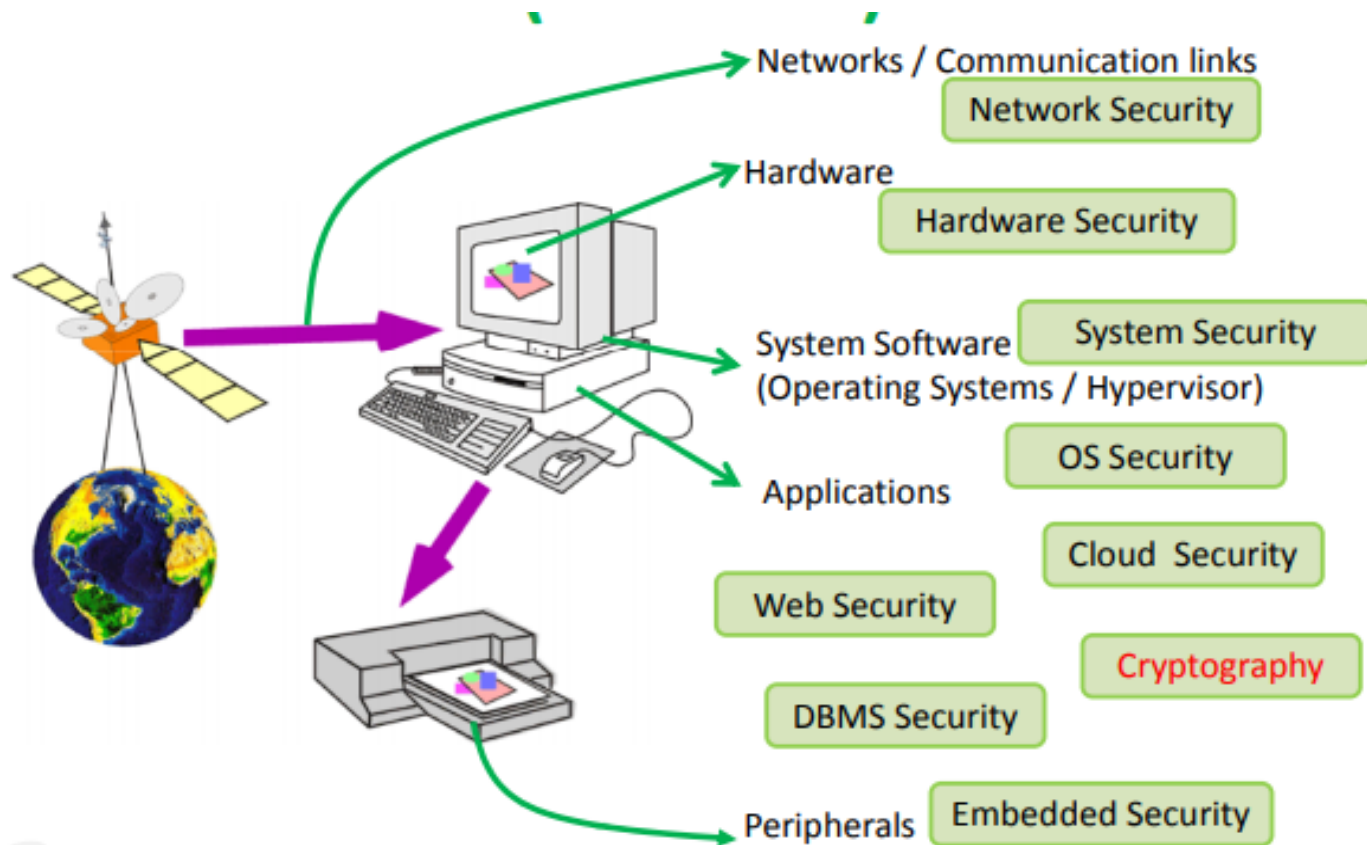
It is predicted that **GLOBAL CYBERSECURITY** spending will exceed **\$1 TRILLION** cumulatively from 2017 to 2021.

Cybersecurity Ventures



VARONIS

Security Studies(an ocean)



Information Security vs. Cyber Security vs. Network Security

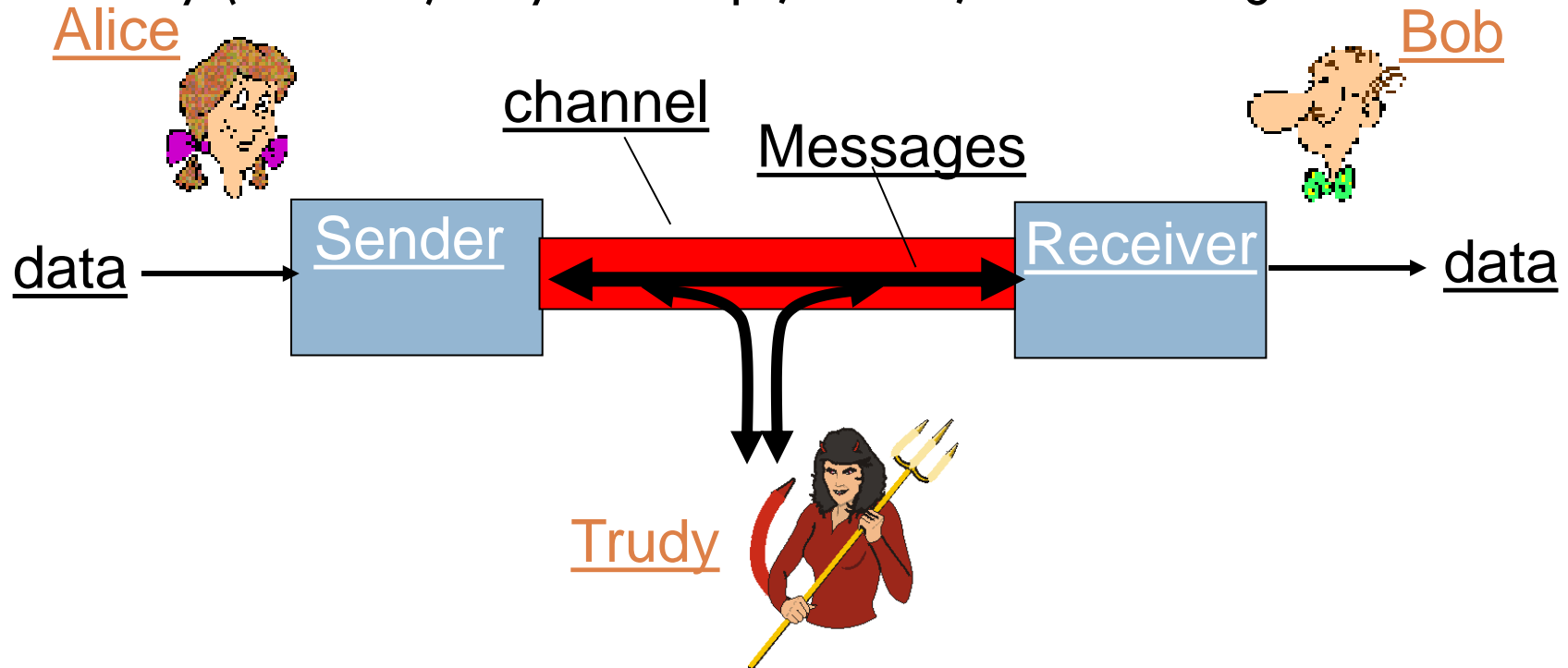
- What is Information Security?
 - ▣ Information security (also known as InfoSec) ensures that both physical and digital data is protected from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction.
 - ▣ Information security differs from cybersecurity in that InfoSec aims to keep data in any form secure, whereas cybersecurity protects only digital data.

Information Security vs. Cyber Security vs. Network Security cont....

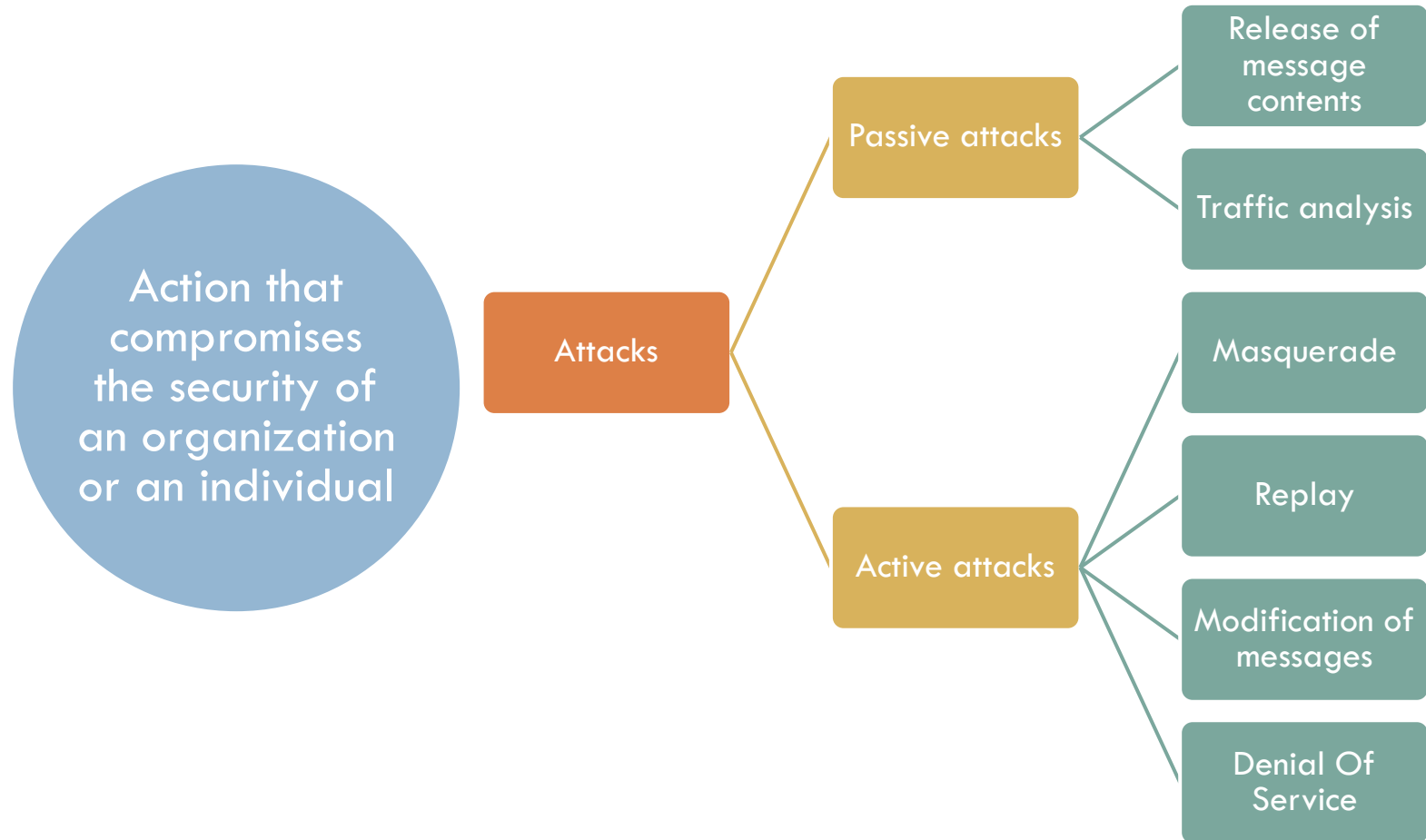
- What is Cybersecurity?
 - ▣ Cybersecurity, is a process or measures taken by organizations or experts to protect devices, computer networks, or data from malicious activities.
- What is Network Security?
 - ▣ a subset of cybersecurity, aims to protect any data that is being sent through devices in your network to ensure that the information is not changed or intercepted.
 - ▣ role of network security is to protect the organization's IT infrastructure from all types of cyber threats.

Communication over the Internet

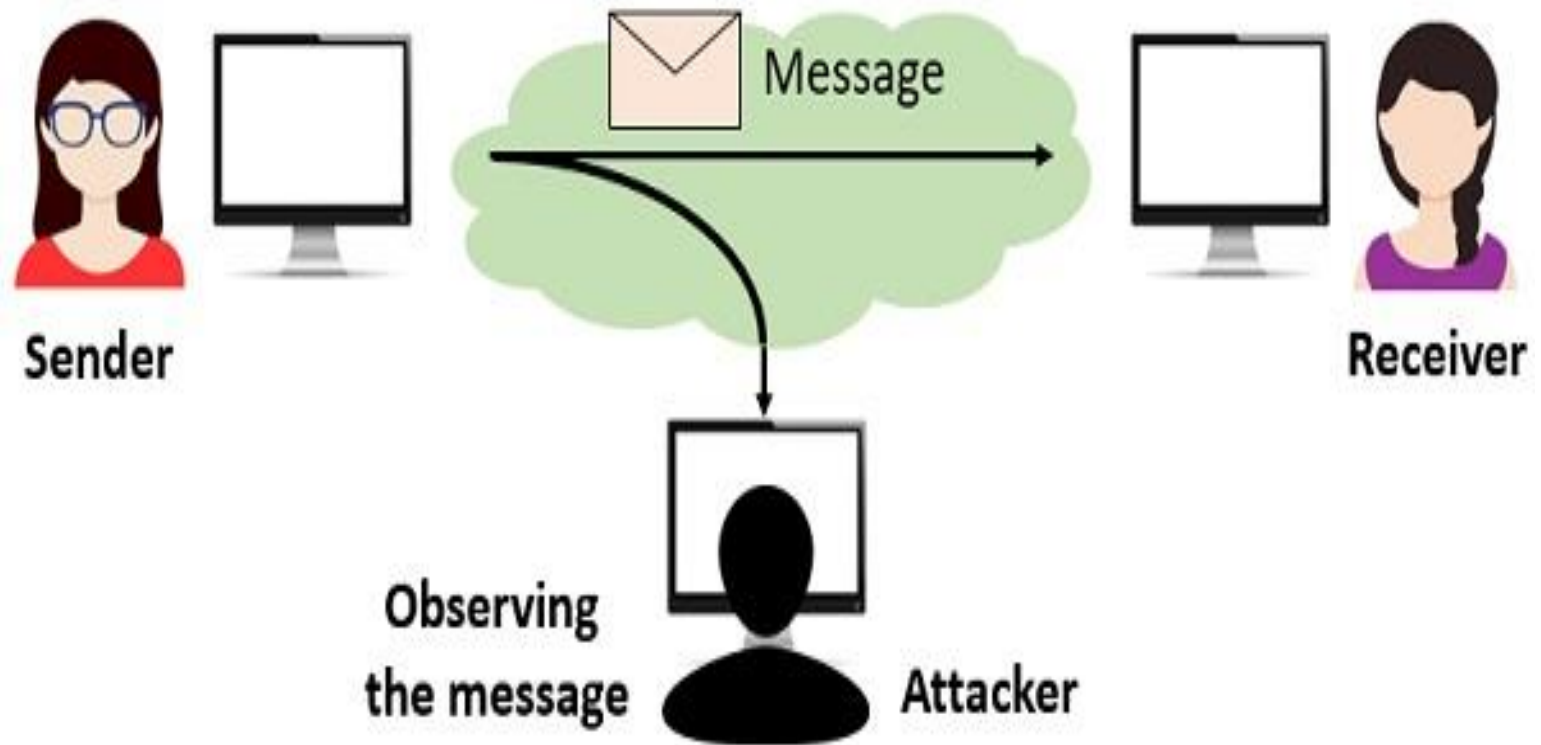
- Friends and enemies: Alice, Bob, Trudy
- well-known in network security world
- Bob, Alice (lovers!) want to communicate “securely”
- Trudy (intruder) may intercept, delete, add messages



Security attacks

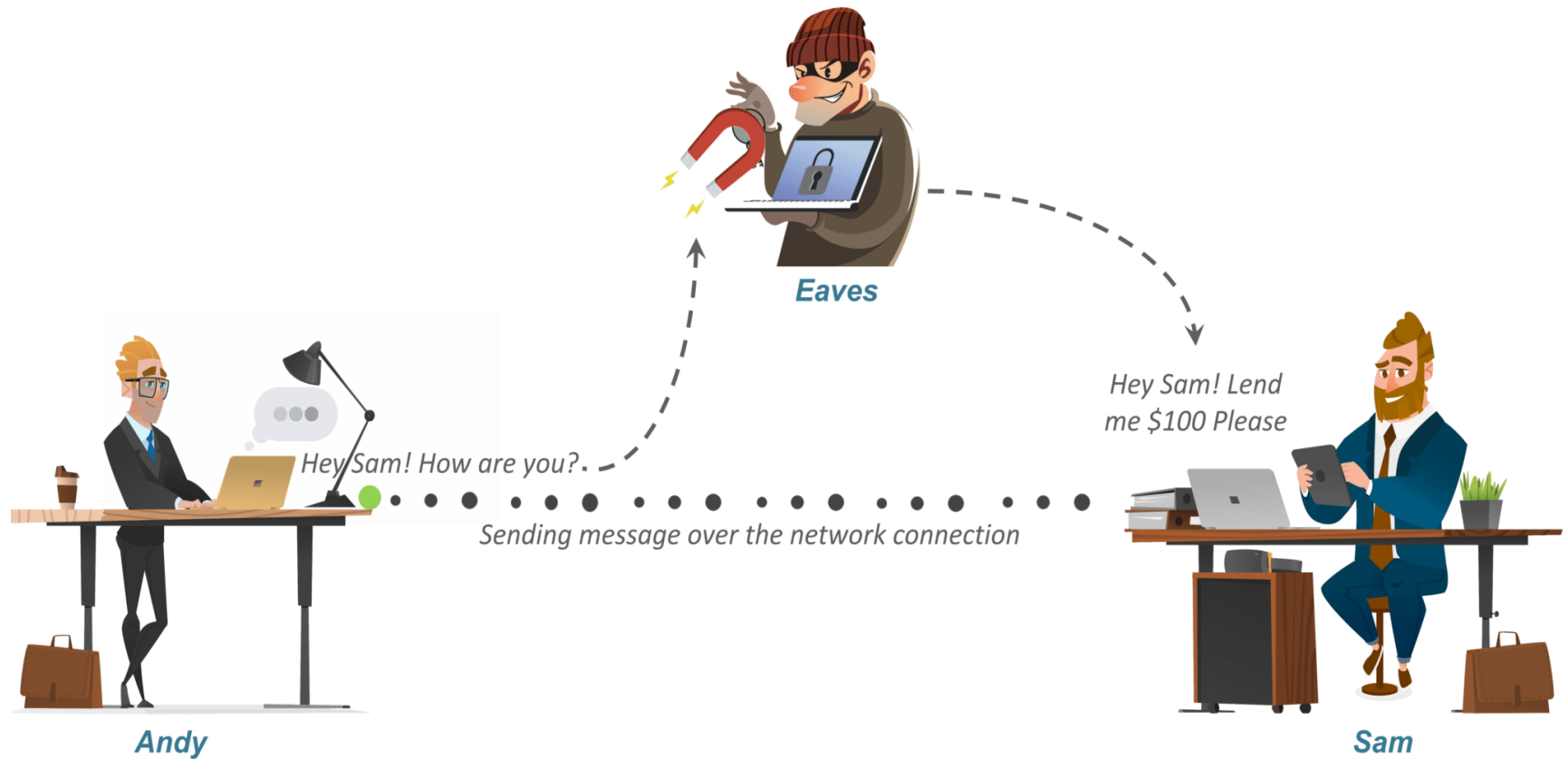


Passive Attacks



Passive Attack

Active attack



Security Attacks

A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*

- A *passive attack* attempts to learn or make use of information from the system but does not affect system resources
- An *active attack* attempts to alter system resources or

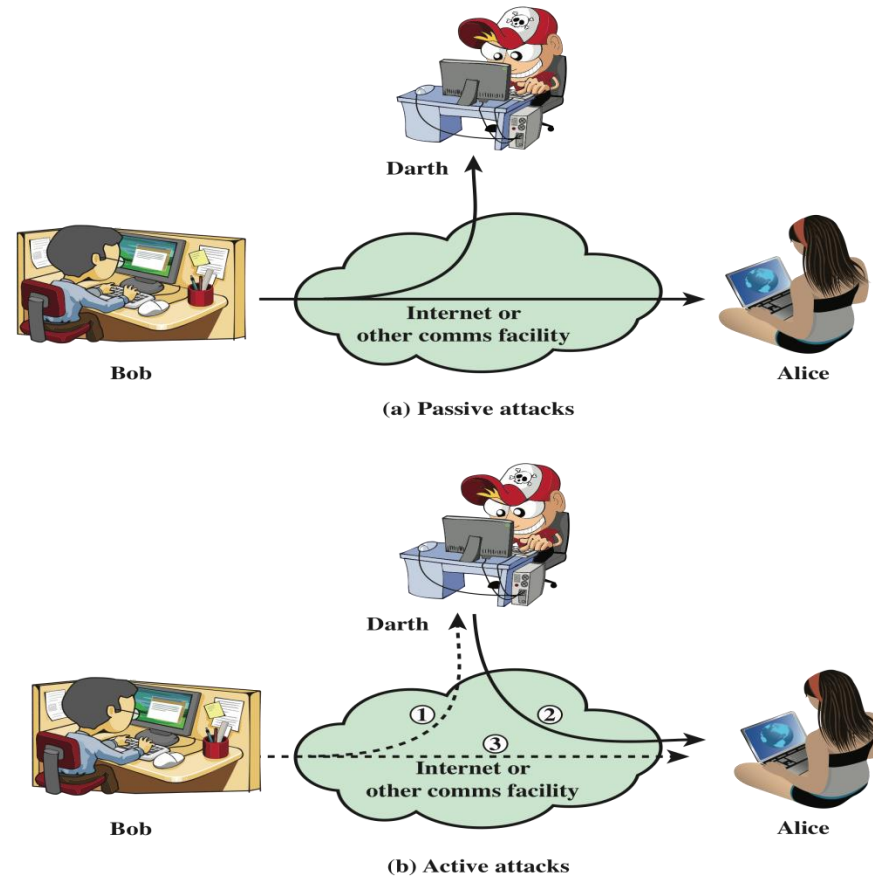


Figure 1.1 Security Attacks

Passive Attacks



- the nature of eavesdropping on, or monitoring of, transmissions
- Goal of the opponent is to obtain information that is being transmitted

- Two types of passive attacks are:
 - ▣ The release of message contents
 - ▣ Traffic analysis

Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them



Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Modification of messages

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Denial of service

- Prevents or inhibits the normal use or management of communications facilities

Security goals-CIA Triad

- Crucial component in all security system: CIA triad
- Cryptography used to achieve:

- Confidentiality

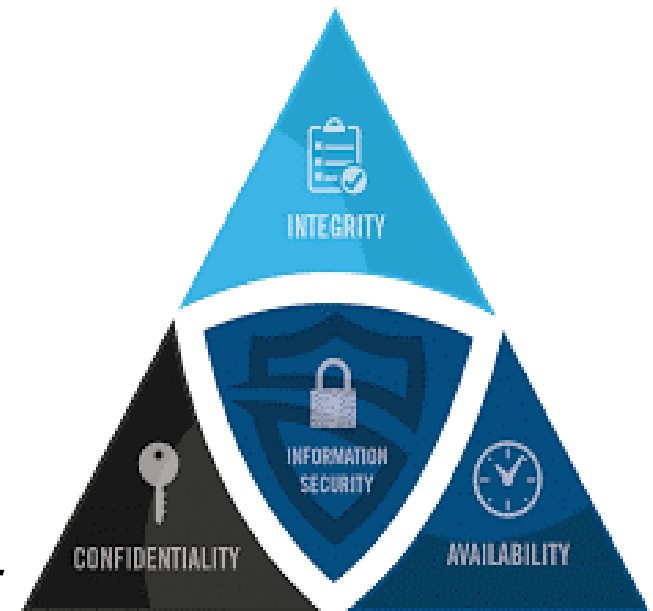
Only authorized users access information

- Integrity

Ensure completeness, accuracy and an absence of unauthorized modifications

- Availability

Available and operational when required by users



need to define some other security objectives!

- **Authentication** - a mechanism (a protocol) by which a user is identified and uses some token to prove who they are.
- **Non-repudiation**- a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

Cryptography

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it.

Thus preventing unauthorized access to information.

The prefix “**crypt**” means “**hidden**” and suffix “**graphy**” means “**writing**”.

Sample Encrypted Message

-----BEGIN PGP MESSAGE-----

Version: GnuPG v2.0.20 (MingW32)

hQEMA5EOTKIA1RLeAQgAk0+I4DzLmyygCxWs/f+R0XjVtJIFp5010gjhcZC5+h58
9vqKZF51ld/+2vi/Jzt6vfSW2ORqPRfkeVcWCzZ4FS6RcHX6d9IkbHENdf6/US+o
IZnqTOx/QIcEvhVqpgEs0iO1yjQ5GyPpUhPwiNchoWcEyjp6p6OjdXSnVXpR8Kw1
6ssbTFIZOx7bO5O0VNH6dExhV9D86OqkGnhE7ap8IH5J8uzUJD1pPdNiRQRTu+Qv
vb30kBQ34egGY5avJKBk88ybtXEbfaWKREbGtZaClkAOXNPjFAEmar/ENx6ceKUF
UzEbJl7j520JFchGEGdpQufzc8IrPAzfW2XnxzZOMdLpAVzyKMr3+SENCsere+vN
K48dKwosb0gIWFPVtWZh7swEtTRiMnyP7NkHB3PlQ3gtx7N04a5yPQJq0JBUoq0E
SlDv5K2q2gSL+HiCj31lDIltMHkbNGtJDP+/4ETgScId9lAKvr6FK9mzLYrp09gz
+Y8g6Lgz+Ib6YWhQuwyG4ObqkIywZeBvtQ5yWLk9HdrOiqpBFhzLcKfs60NzWUNd
cZIELVn7cqsSlIYBw0CtqAb80vrX6zxIS6MTjNzIwQGwcbH0uaA3ctgGbnF7/E0n
sx8jBCA/8+nACuR3ZEmDqrhCZRvHEUWgo7tBa4Hi8oJ3JaxiO3xMJmulsN2PDyg/
dj+AG6hVJidNBdvBQmFOCdcDTAaBSMPxHeZQeEKoHXG6l7QQr9ZsHuN+1+tRPTZy
ldXWZwcZ9Ei55+vO2xwIjVpYfjQT11qofHbVofTn61LSVuLtTnLDP+pVW6tmalai
zGrqrBK9gm0A7XqIpIF7LqurDVODH0+NvYC75xQwHPOQ7An9P8JUvjmWUbPEZsBJ
1mwb3weQ9WorCYHX2SC16gTLFaKAvyRZyCkiVdy2HZQJFnOuCtXN49Kwr37zcam2
Ic9+8IwQcEzwcMO+0W1VumPsTTglNWEXu5JQ1OZC2Oa+6laa5XxbmV0b059P25O+
gKpfQUgVNUF0IicVYCEzH+cZjZ8+JtL+Wil07gsQAYa4w/eP/nRQXKVgA==
=ZZ4U

-----END PGP MESSAGE-----

German Telegram

CLASS OF SERVICE DESIRED	
Fast Day Message	<input checked="" type="checkbox"/>
Day Letter	<input type="checkbox"/>
Night Message	<input type="checkbox"/>
Night Letter	<input type="checkbox"/>

Patrons should mark, as X, opposite the class of service desired. OTHERWISE, THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Receiving No.	15
Check	5550
Time Filed	

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

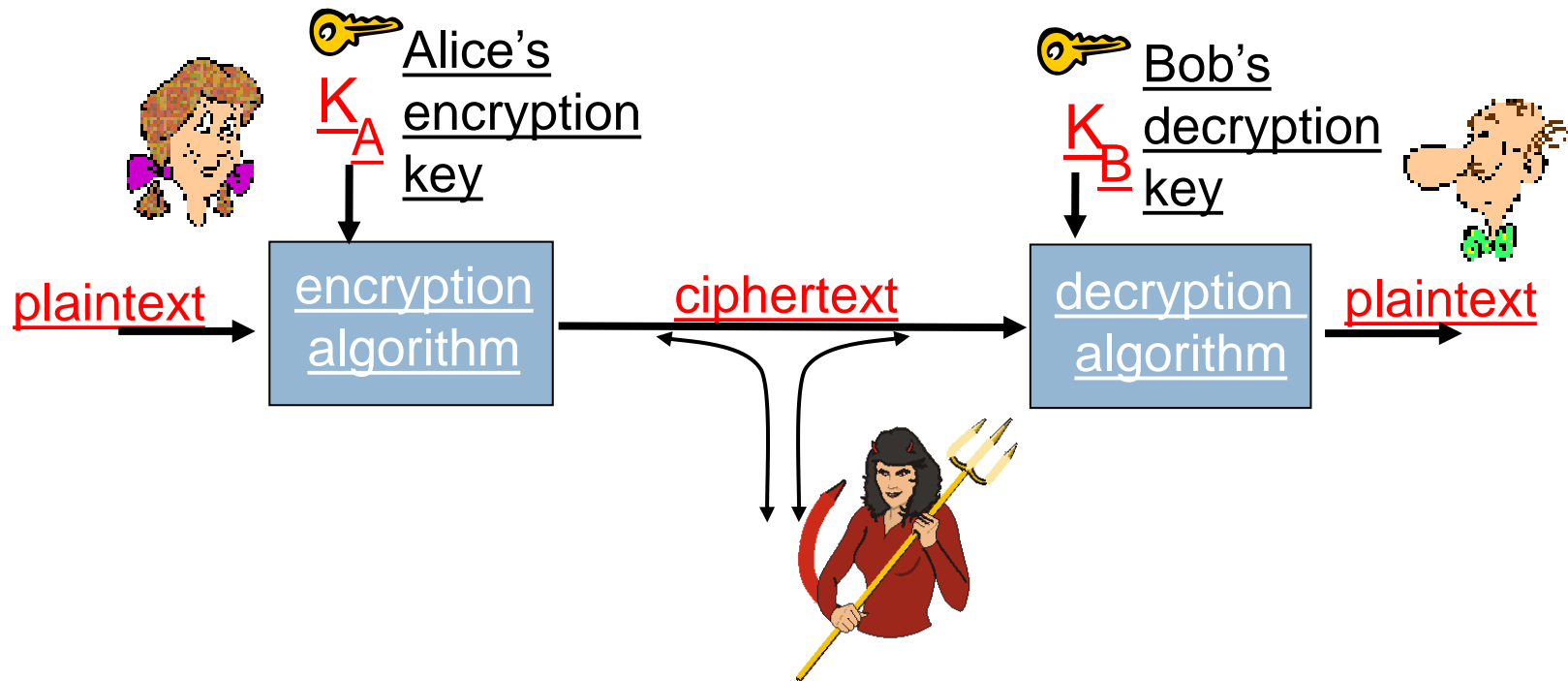
130	13042	13401	8501	115	3528	416	17214	6491	11310
18147	18222	21560	10247	11518	23677	13605	3494	14936	
98092	5905	11311	10392	10371	0302	21290	5161	39695	
23571	17504	11269	18276	18101	0317	0228	17694	4473	
22284	22200	19452	21589	67893	5569	13918	8958	12137	
1333	4725	4458	5905	17166	13851	4458	17149	14471	6706
13850	12224	6929	14991	7382	15857	67893	14218	36477	
5870	17553	67893	5870	5454	16102	15217	22801	17138	
21001	17388	7446	23638	18222	6719	14331	15021	23845	
3156	23552	22096	21604	4797	9497	22464	20855	4377	
23610	18140	22260	5905	13347	20420	39689	13732	20667	
6929	5275	18507	52262	1340	22049	13339	11265	22295	
10439	14814	4178	6992	8784	7632	7357	6926	52262	11267
21100	21272	9346	9559	22464	15874	18502	18500	15857	
2188	5376	7381	98092	16127	13486	9350	9220	76036	14219
5144	2831	17920	11347	17142	11264	7667	7762	15099	9110
10482	97556	3569	3670						

BEPNSTORFF.

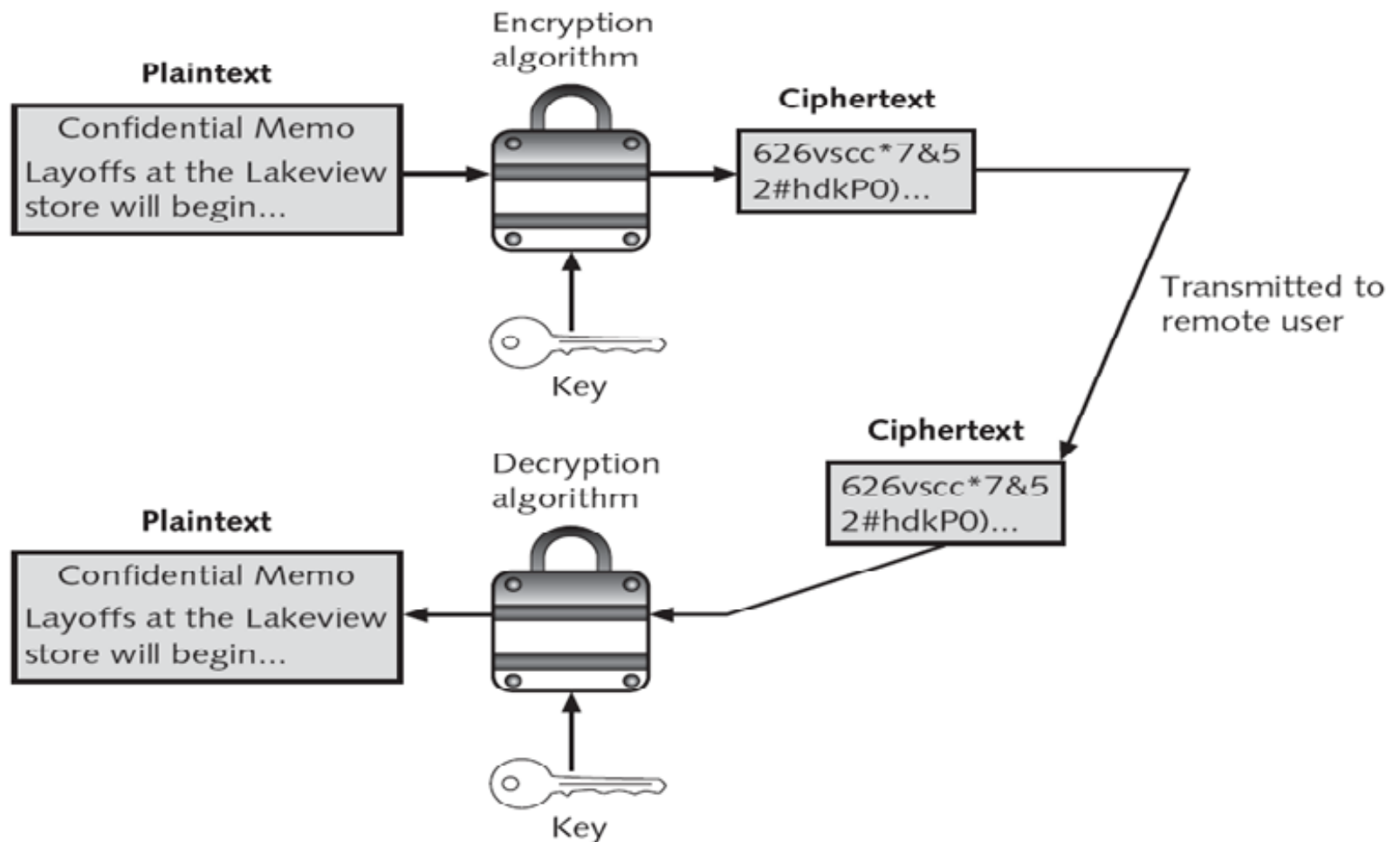
Charge German Embassy.

862.2019/724

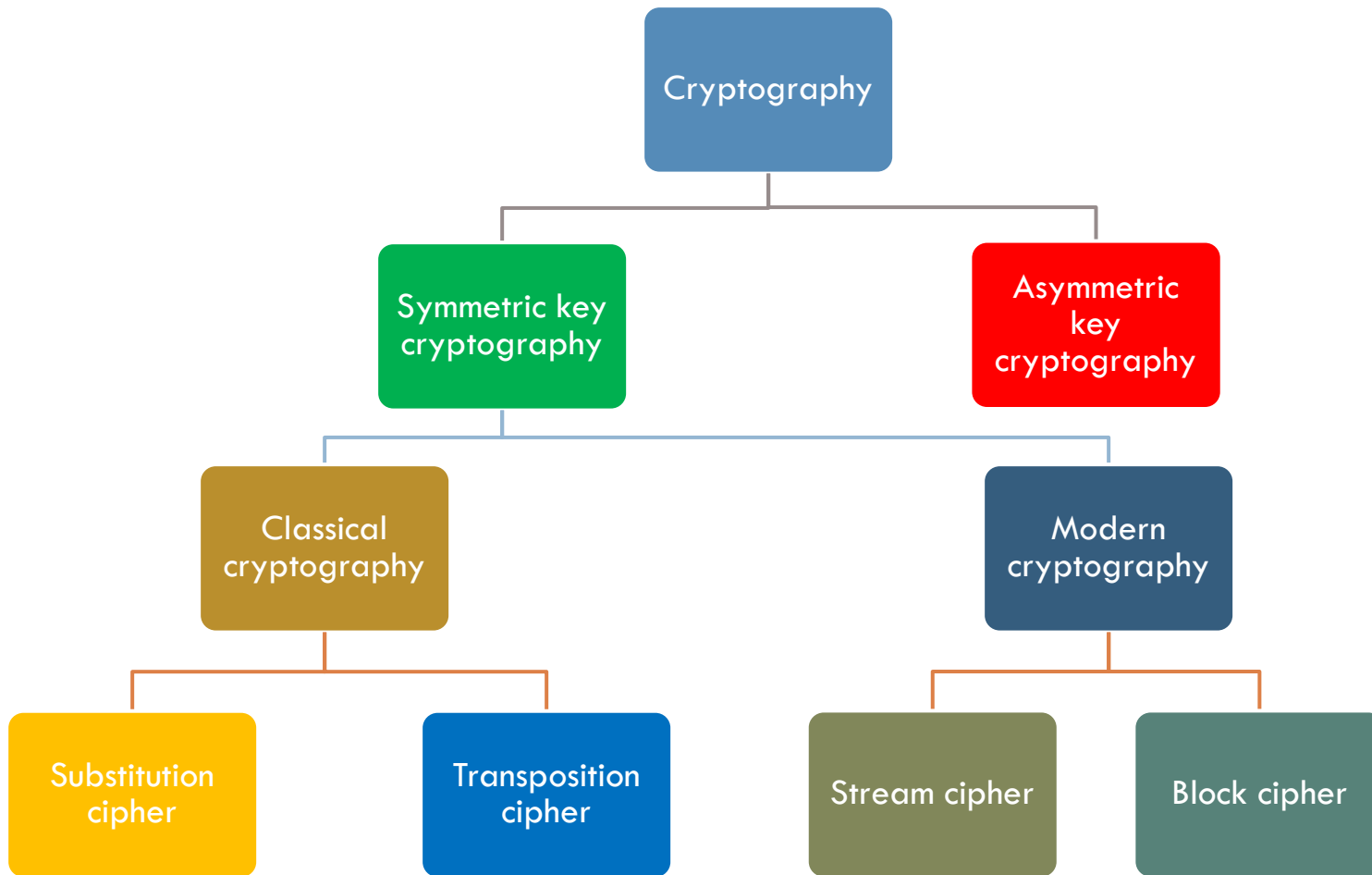
The language of cryptography



Cryptographic process



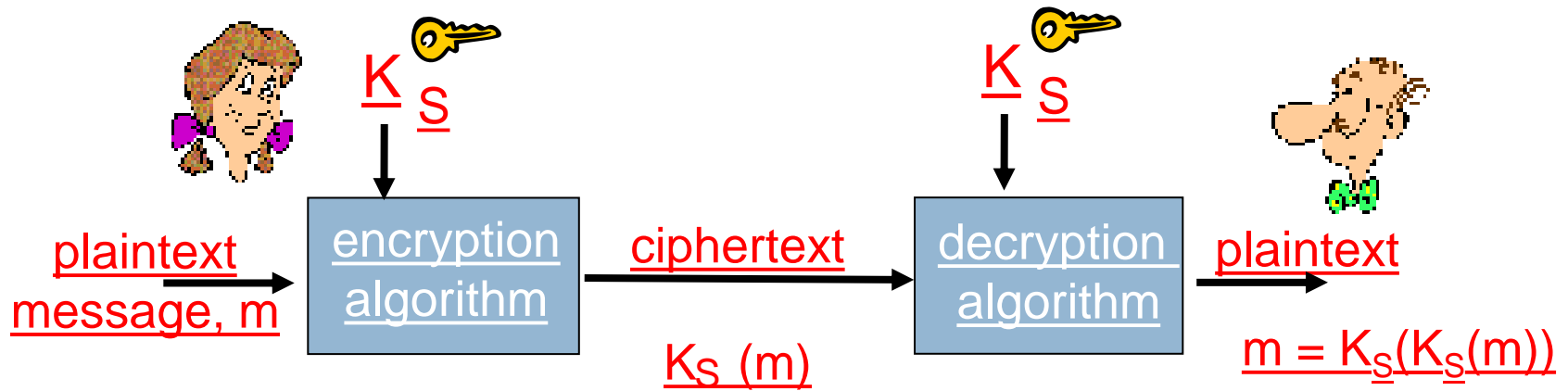
Classification of Cryptography



Types of Cryptography

- Crypto often uses keys:
 - ▣ Algorithm is known to everyone
 - ▣ Only “keys” are secret
- Symmetric key cryptography
 - ▣ Involves the use one key
- Asymmetric key/Public key cryptography
 - ▣ Involves the use of two keys

Symmetric key cryptography



symmetric key crypto: Bob and Alice share same (symmetric) key: K

The most common symmetric key system is the Data Encryption Standard (DES)

Substitution Cipher: Caesar Cipher

MESSAGE FROM MARY STUART KILL THE QUEEN

Substitution Table - Caesar's Cipher

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

key = 3 cyclic shifts



PHVVD JHIUR PPDUB VWXDU WNLOO WKHTX HHQ

General Substitution Table

ABCDEFGHIJKLMNOPQRSTUVWXYZ

EYUOBMDXVTHIJPRCNAKQLSGZFW

26! possible keys

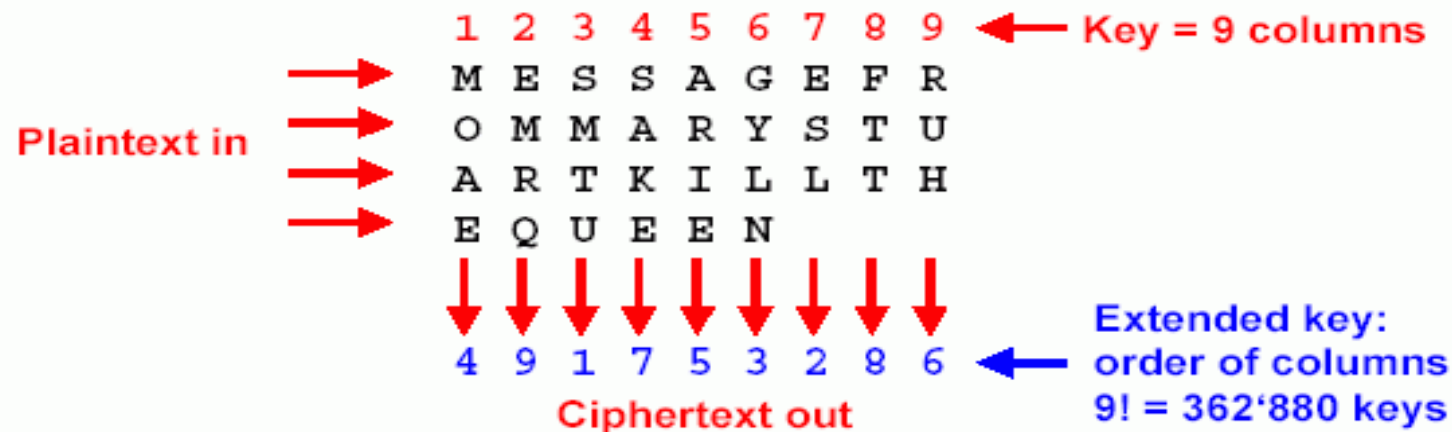
Courtesy:
Andreas
Steffen

JBKKE DBMAR JJEAF KQLEA QHVII QXBNL BBP

Modern substitution ciphers take in N bits and substitute N bits using lookup table: called S-Box

Transposition cipher

MESSAGE FROM MARY STUART KILL THE QUEEN



MOAEE MRQSM TUSAK EARIE GYLNE SLFTT RUH
SMTUE SLGYL NMOAE ARIER UHSAK EFTTE MRQ

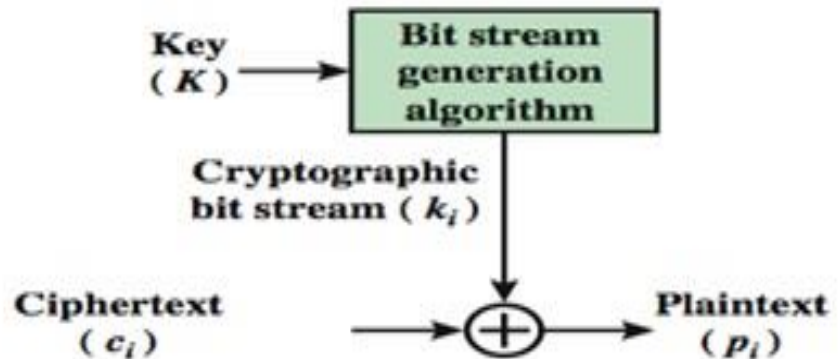
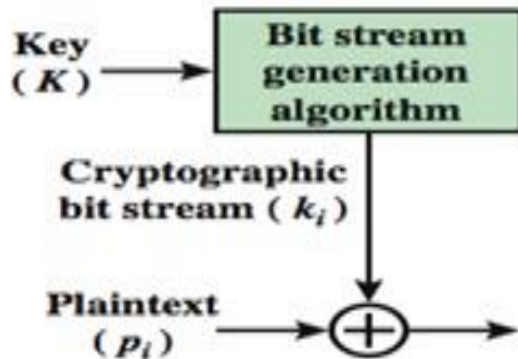
Courtesy:
Andreas
Steffen

Diffusion means permutation of bit or byte positions !

Modern Transposition ciphers take in N bits and permute using lookup table : called P-Boxes

Stream Cipher

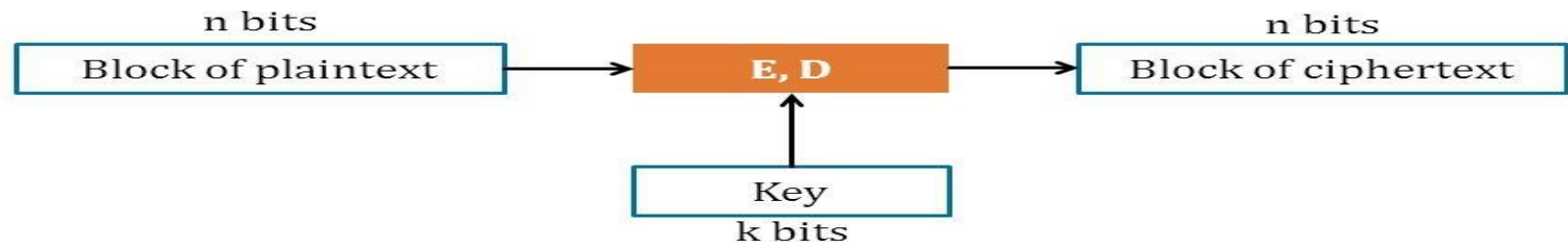
- Combine each bit of keystream with bit of plaintext to get bit of ciphertext
 - ▣ $c(i) = ks(i) \oplus m(i)$
 - ▣ $m(i) = ks(i) \oplus c(i)$



(a) Stream Cipher Using Algorithmic Bit Stream Generator

Block ciphers

- Message to be encrypted is processed in blocks of k bits (e.g., 64-bit blocks).



1. 3DES: $n = 64$ bits, $k = 168$ bits
2. AES: $n = 128$ bits, $k = 128, 192, 256$ bits



Thank You...
Any queries...?

manik.chavan@walchandsangli.ac.in