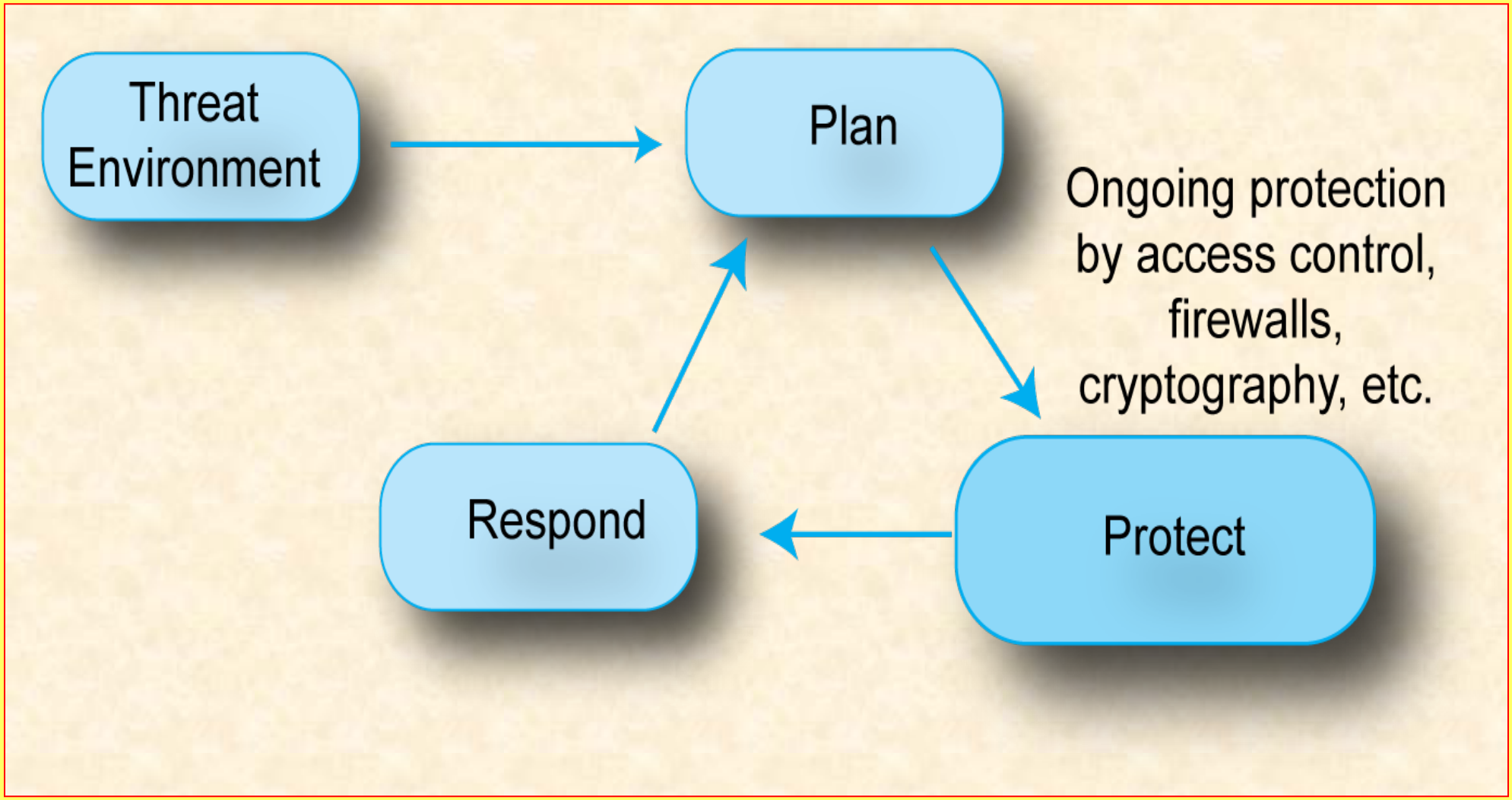
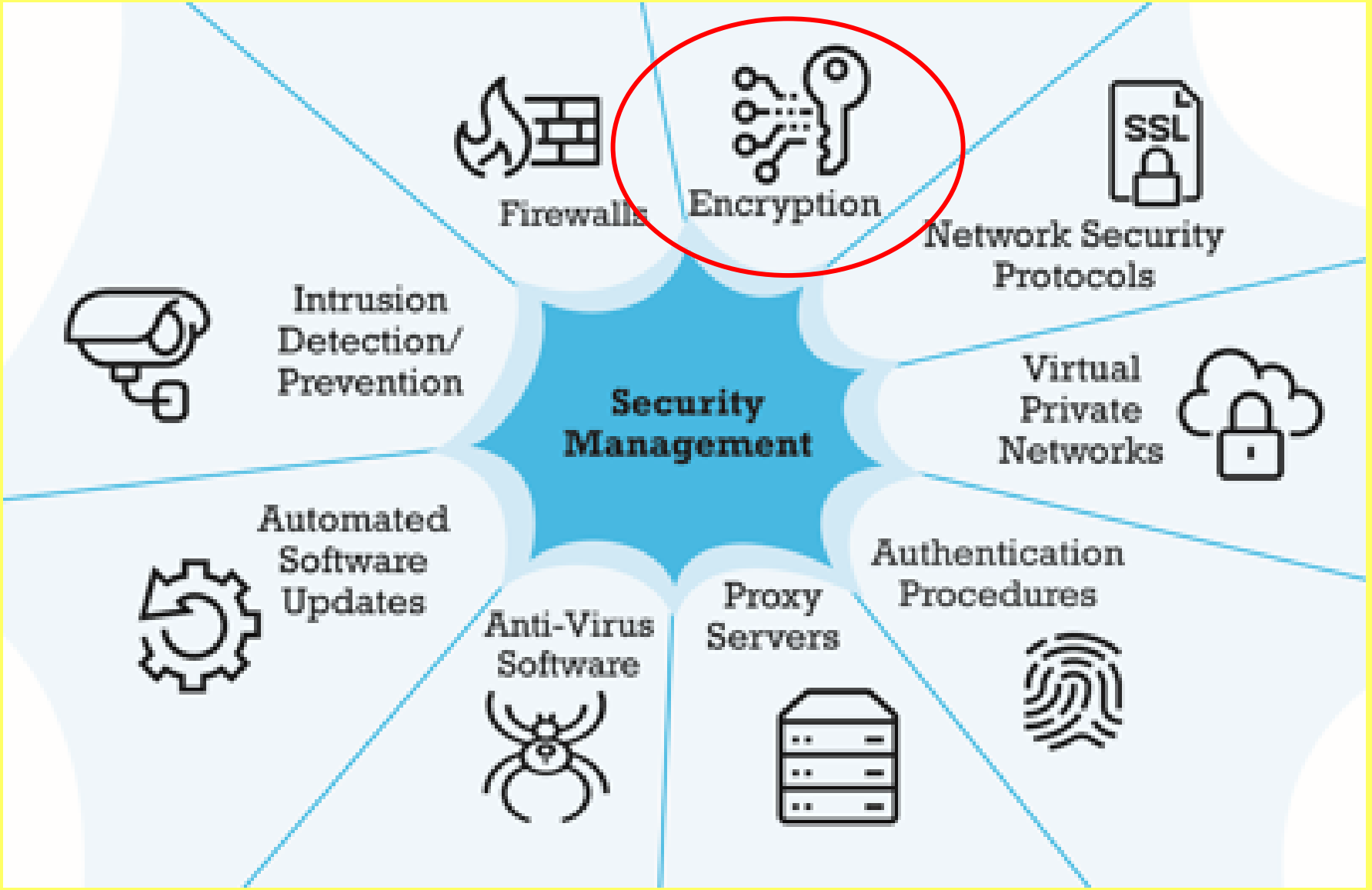
EE 8084

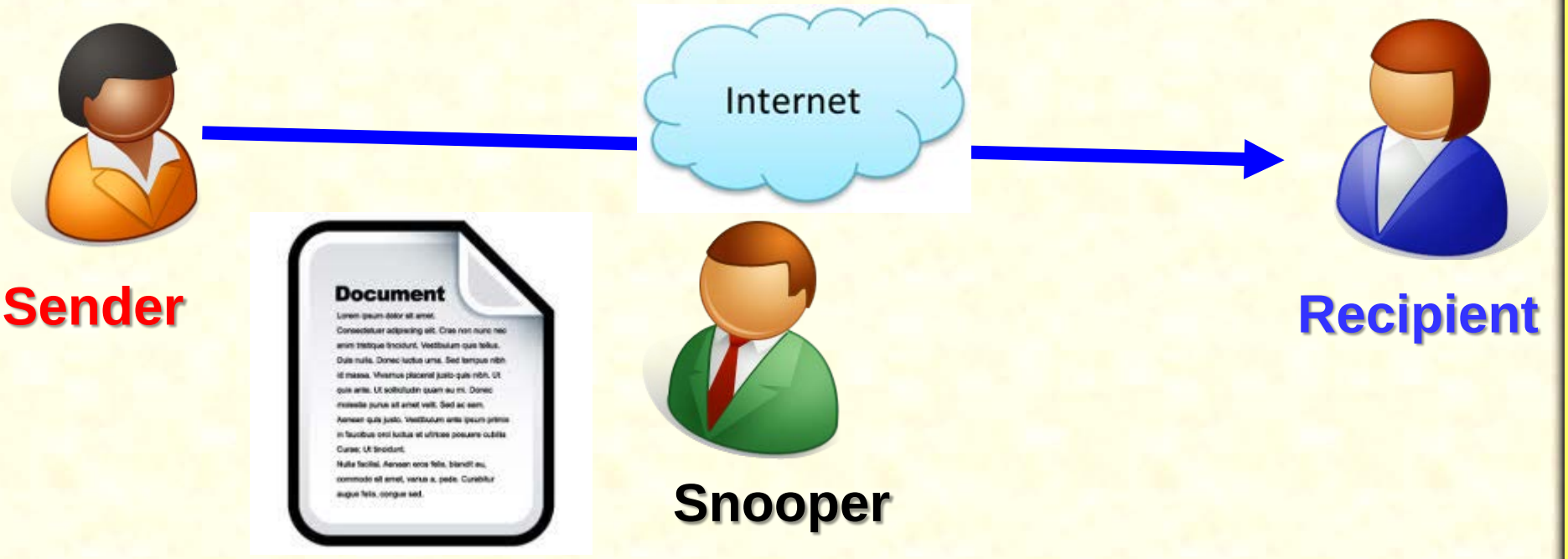
CYBER SECURITY


Threat Environment
Plan
Ongoing protection by access control, firewalls, cryptography, etc.
Protect
Respond


Firewalls
Encryption
SSL
Network Security Protocols
Intrusion Detection/ Prevention
Security Management
Virtual Private Networks
Automated Software Updates
Anti-Virus Software
Proxy Servers
Authentication Procedures

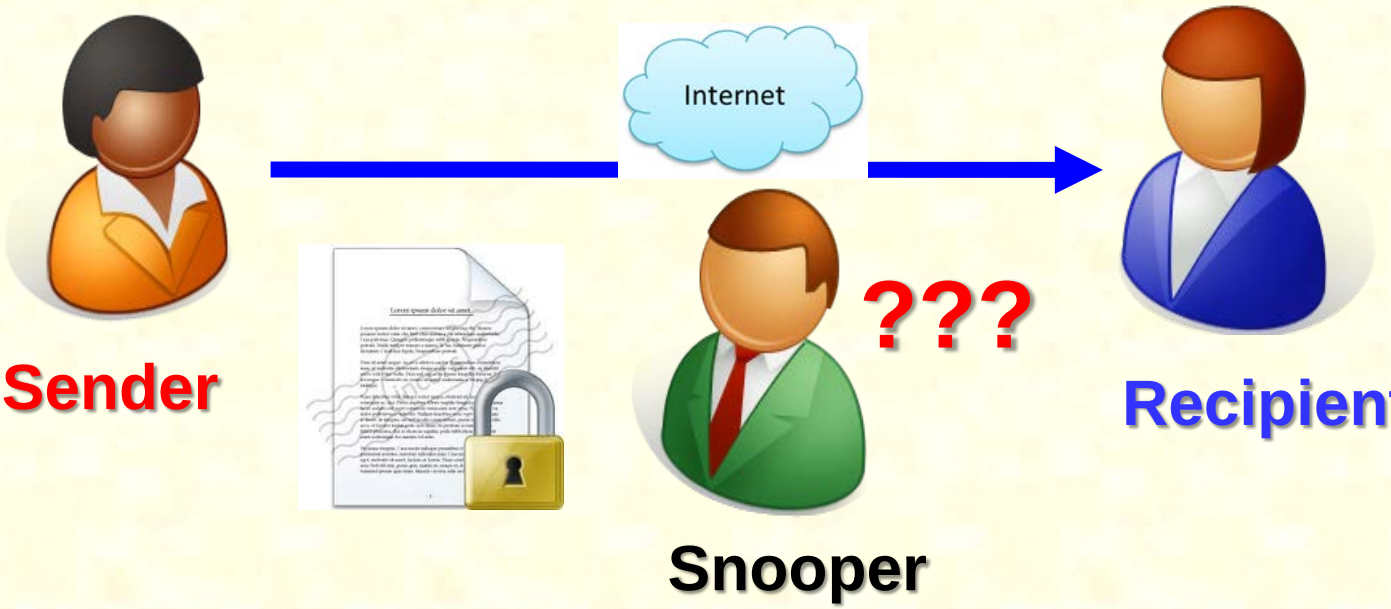
CRYPTOGRAPHY

OPEN COMMUNICATIONS



CRYPTOGRAPHY

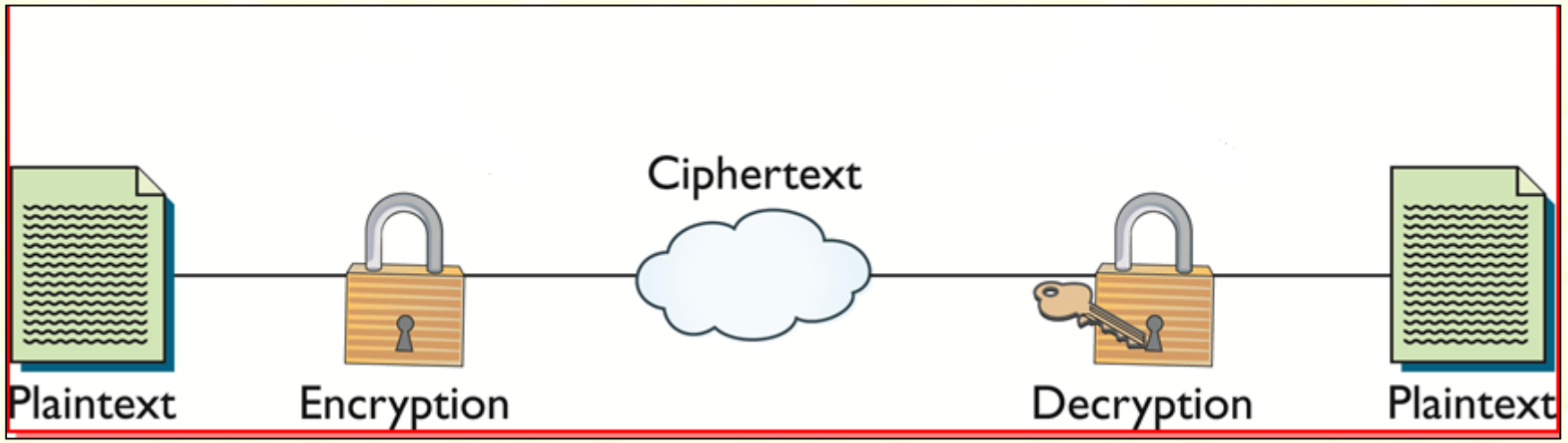
- Greek kryptós (hidden) and gráphien (to write)
- The study of ways to hide or obscure information, making it unreadable without secret knowledge
- Cryptography is the use of mathematical operations to protect messages traveling between parties or stored on a computer
- It means that someone intercepting your communications cannot read them



CRYPTOGRAPHY

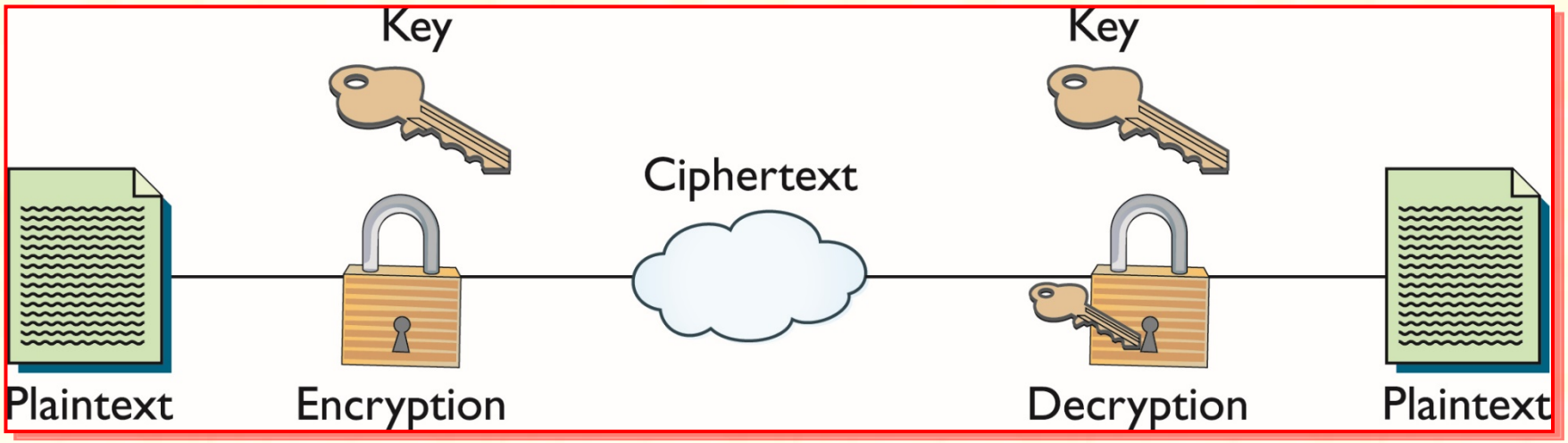
- **CRYPTOGRAPHY:** is the art and science of secret writing, encrypting, or hiding of information from all but the intended recipient.
- **CRYPTANALYSIS:** is the process of attempting to break a cryptographic system and return the encrypted message to its original form.
- **BASIC DEFINITIONS**
  - **PLAINTEXT**: A piece of data that is not encrypted
  - **CIPHERTEXT**: The output of an encryption algorithm
  - **CIPHER**: A cryptographic algorithm
  - **KEY**: A sequence of characters or bits used by an algorithm to encrypt or decrypt a message
  - **ENCRYPTION**: Changing plaintext to ciphertext
  - **DECRYPTION**: Changing ciphertext to plaintext

ENCRYPTION AND DECRYPTION PROCESS



- **NOTATION**
  - **M** = Message, **C** =ciphertext, **E**= encryption, **D** = decrypting
  - E(M) = C (encrypting message = ciphertext)
  - D(C) = M (decrypting ciphertext = message)

ENCRYPTION AND DECRYPTION PROCESS



- **NOTATION USING A KEY**
- **Secret-key (Symmetric) cryptosystem – one key**
  - $E_K(M) = C$ $D_K(C) = M$
- **Public-key (Asymmetric) cryptosystem – two keys**
  - $E_{K1}(M) = C$ $D_{K2}(C) = M$

CRYPTOGRAPHY

- **CRYPTOGRAPHIC ALGORITHMS**
  - The cryptographic algorithm—what is commonly called the encryption algorithm or cipher—is made up of mathematical steps for encrypting and decrypting information.
- **TYPES OF CIPHERS**
  - **Substitution** ciphers (replace)
  - **Transposition** ciphers (rearrange)
  - **Product ciphers** (substitution, permutation, and modular arithmetic)
  - Vigenère
  - One-time pad
- **KEYS**
  - Keys are special pieces of data used in both the encryption and decryption processes.
  - The algorithms stay the same, but a different key is used.
  - The more complex the key, the greater the security of the system.

KEY LENGTH

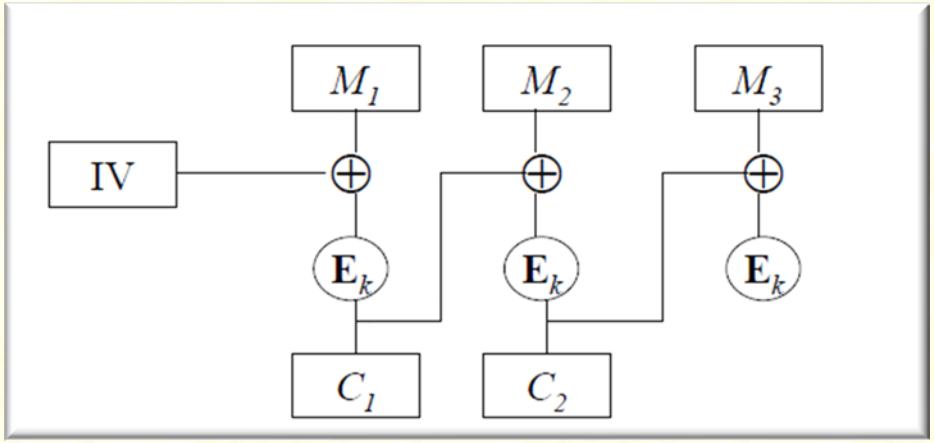
- **SECURITY = STRENGTH OF ALGORITHM + LENGTH OF KEY**
- Key of 8 bits has 2^8 or 256 possible combinations. Trivial to break even without a computer (50% chance of finding the key after 128 tries)
- Every bit you add, doubles the number of possible combinations.
- Assuming a key of 56 bits, there are 2^{56} possible combinations.
  - If a computer can try 1,000,000 keys a second, it would take (2^{56}/1,000,000*365*24*60*60) 2285 years to find the correct key.
  - A 64-bit key would take 585,000 years.
  - 128 bits requires 10^{25} years.
  - However, computers are much faster than 1M keys/s these days and with hackers using millions of compromised computers in parallel, in reality it is much easy to break it then it is in theory.

CRYPTOGRAPHY

- Plaintext can be encrypted through stream cipher or block cipher method
- **STREAM CIPHER:** A typical stream cipher encrypts plaintext one byte at a time, although a stream cipher may be designed to operate on one bit at a time or on units larger than a byte at a time.
- Processes the input elements continuously
- Produces output one element at a time
- Primary advantage is that they are almost always faster and use far less code.
- For applications that require encryption/decryption of a stream of data, such as over a data communications channel or a browser/Web link, a stream cipher might be the better alternative.
- RC4, is the most widely used of all stream ciphers.
- It was developed in 1987 by Ron Rivest, one of the developers of the public-key cipher RSA.
- **BLOCK CIPHER:** Message divided into blocks (e.g., sets of 8- or 16-bit blocks) and each is transformed into encrypted block of cipher bits using algorithm and key.

CRYPTOGRAPHY

- A block cipher processes the input one block of elements at a time, producing an output block for each input block.
- For applications that deal with blocks of data, such as file transfer, e-mail, and database, block ciphers may be more appropriate.
- Examples of block cipher are, DES, 3DES, AES, RC5, Blowfish etc.
- **ENCRYPTION MODES:** Different encryption modes may be used. Common modes are:
  - **Electronic Code Book (ECB):** Each block encrypted separately.
  - **Cipher Block Chaining (CBC):** Next input depends on previous output



CRYPTOGRAPHY

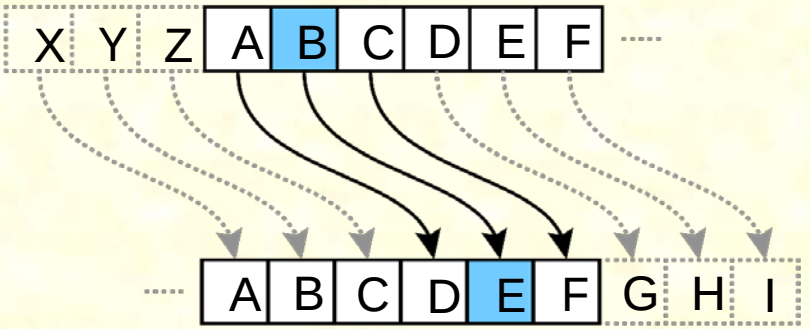
- **CRYPTOSYSTEM:** (or Cryptographic system) is the package of all procedures, protocols, cryptographic algorithms and instructions used for enciphering and deciphering messages using cryptography.
- **CHOOSING ALGORITHMS**
- **Depends on the application**
  - Encrypting streams of data in real-time has different requirements than encryption files on your local computer
  - **SYMMETRIC:** Best for data on your hard drive
  - **PUBLIC:** Good for messages
- **Cryptography is Used to Achieve Information**
  - **CONFIDENTIALITY**: only authorized persons can access information
  - **INTEGRITY**: Information that was sent is what was received
  - **AUTHENTICATION**: Guarantee of originator and of electronic transmission (using digital signature)
  - **NON-REPUDIATION:** Originator of information cannot deny content or transmission (using digital signature)

SHIFT OR CAESAR'S CIPHER

- Caesar's cipher uses an algorithm and a key
  - The algorithm specifies that you offset the alphabet either to the right (forward) or to the left (backward)
  - The key specifies how many letters the offset should be.
- The Caesar's cipher is also known as a shift cipher.
- Historically, **additive ciphers** are called shift ciphers.
- **Julius Caesar** used an additive cipher to communicate with his officers.
- For this reason, additive ciphers are sometimes referred to as the Caesar cipher.
- Caesar used a key of 3 for his communications.
- The action of a Caesar cipher is to replace each plaintext letter with one fixed number of places down the alphabet.
- This example is with a shift of three,

so that a **B** in the plaintext becomes

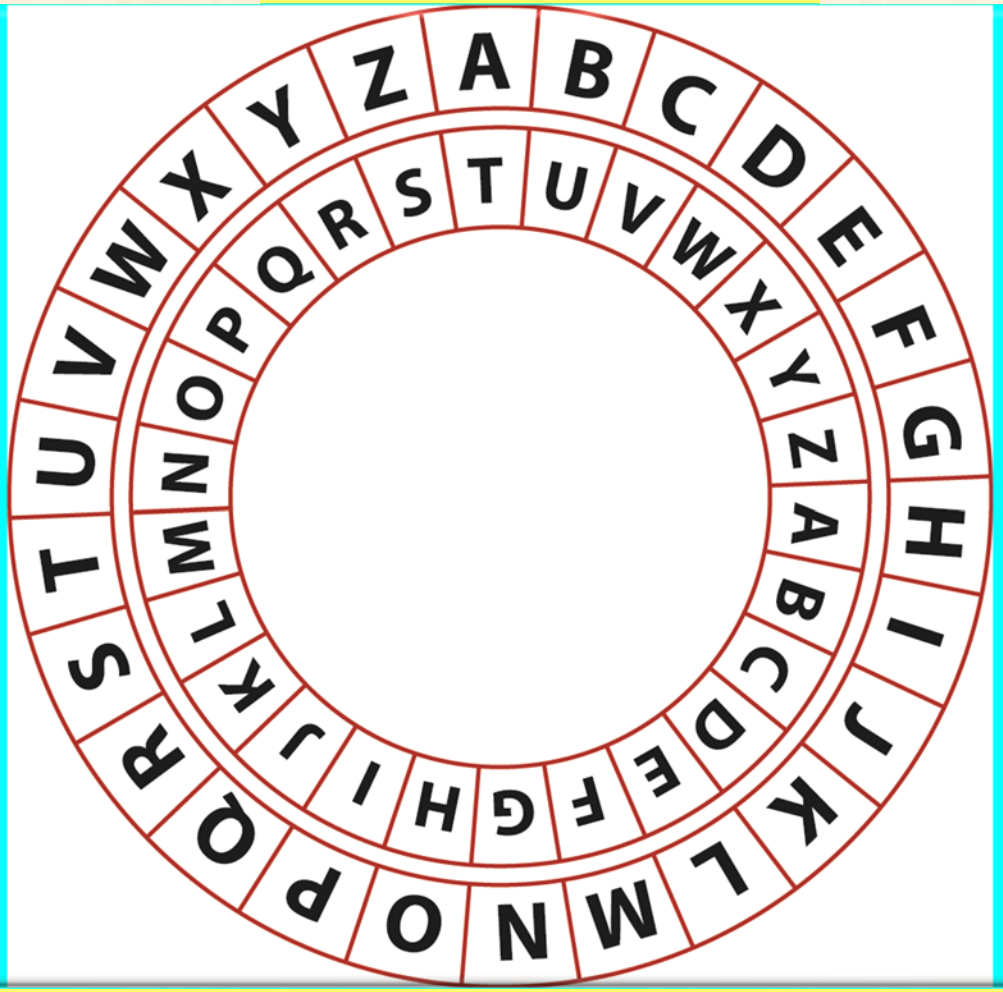
E in the ciphertext.



SHIFT CIPHER EXAMPLE

Solve this:
LPHKWYBLA

Solution
SWORDFISH



SUBSTITUTION CIPHERS

- Simple Shift ciphers are easy to crack.
  - Simply figure out the number of rotations.
- Substitution ciphers were developed because they are more complex.
- Substitution ciphers work on the principle of substituting a different letter for every letter.
  - a becomes g, b becomes d, and so on.
  - The letters are not in order as they are in shift ciphers.
- **BASIC IDEA** –substitute each block of plaintext by a different block.
- If plaintext is English then
  - **Mona-alphabetic** substitution (one to one relationship).
  - **Poly-alphabetic** substitution (one to many relationship).
- If plaintext is binary string then map one block of bits to another.
  - **Plaintext**: 0011010101010001 …10100101
  - **Ciphertext**: 0100010000011100 …00101001

SUBSTITUTION CIPHERS

- In substitution cipher, the alphabets may be shifted, reversed or scrambled
  - **SHIFTED:** Creating the Caesar Cipher
  - **REVERSED:** Creating Atbash cipher (simple substitution cipher for the Hebrew alphabet)
  - **SCRAMBLED**: Creating a mixed alphabet or deranged alphabet.
- Traditionally, mixed alphabets may be created by first writing out a keyword, removing repeated letters in it, then writing all the remaining letters in the alphabet in the usual order.
- **EXAMPLE**: The keyword "zebras" gives us the following alphabets.

Plaintext alphabet:	**ABCDEFGHIJKLMNOPQRSTUVWXYZ**
Ciphertext alphabet:	**ZEBRASCDFGHIJKLMNOPQTUVWXY**

- **A message of:** flee at once. we are discovered!
- **Enciphers to:** **SIAA ZQ LKBA. VA ZOA RFPBLUAOAR!**

TRANSPOSITION CIPHER

- The order of the letters are changed. This can be done at the bit level or at the byte (character) level - transposition ciphers move these bits or bytes to another location in the block, so that bit 1 becomes bit 4, bit 2 becomes bit 7 etc.
- **EXAMPLE:** "THE UNEXAMINED LIFE IS NOT WORTH LIVING" ,Written vertically over six columns becomes:

```
TX SOV
HAL RI
EMINTN
 IFOHG
UNET
NE  L
EDIWI
```

Then, written horizontally becomes:

TX SOVHAL RIEMINTN IFOHGUNET NE LEDIWI

VIGENÈRE CIPHER

- The Vigenère cipher is a much more complex cipher.
- It corrects the issues with more simplistic keys.
- It works as a poly-alphabetic substitution cipher that depends on a password.
  - Makes the algorithms rather simple
  - But the key rather complex, with the best keys comprising very long and very random data
- A Vigenère cipher is done by setting up a substitution table like this one:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

(etc.)

VIGENÈRE CIPHER

- The password is matched up to the text it is meant to encipher.
- The cipher letter is determined by use of the grid
  - Matching the plaintext character's row
  - With the password character's column,
  - Resulting in a single ciphertext character where the two meet.
- For example – Plain text is "Send Help" and the password is "cabinet."
  - 1st plaintext letter S (column), 1st password letter c (row)
  - Ciphertext is now U

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	**S**	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	**U**	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

(etc.)

EXCLUSIVE OR (XOR)

- Function of Boolean algebra; two bits are compared, and binary result is generated.
- If two bits are identical, the result is binary 0.
- If two bits are not identical, the result is binary 1.
- Very simple to implement and simple to break; should not be used by itself when organization is transmitting/storing sensitive data

First bit	Second bit	Result
0	0	0
0	1	1
1	0	1
1	1	0

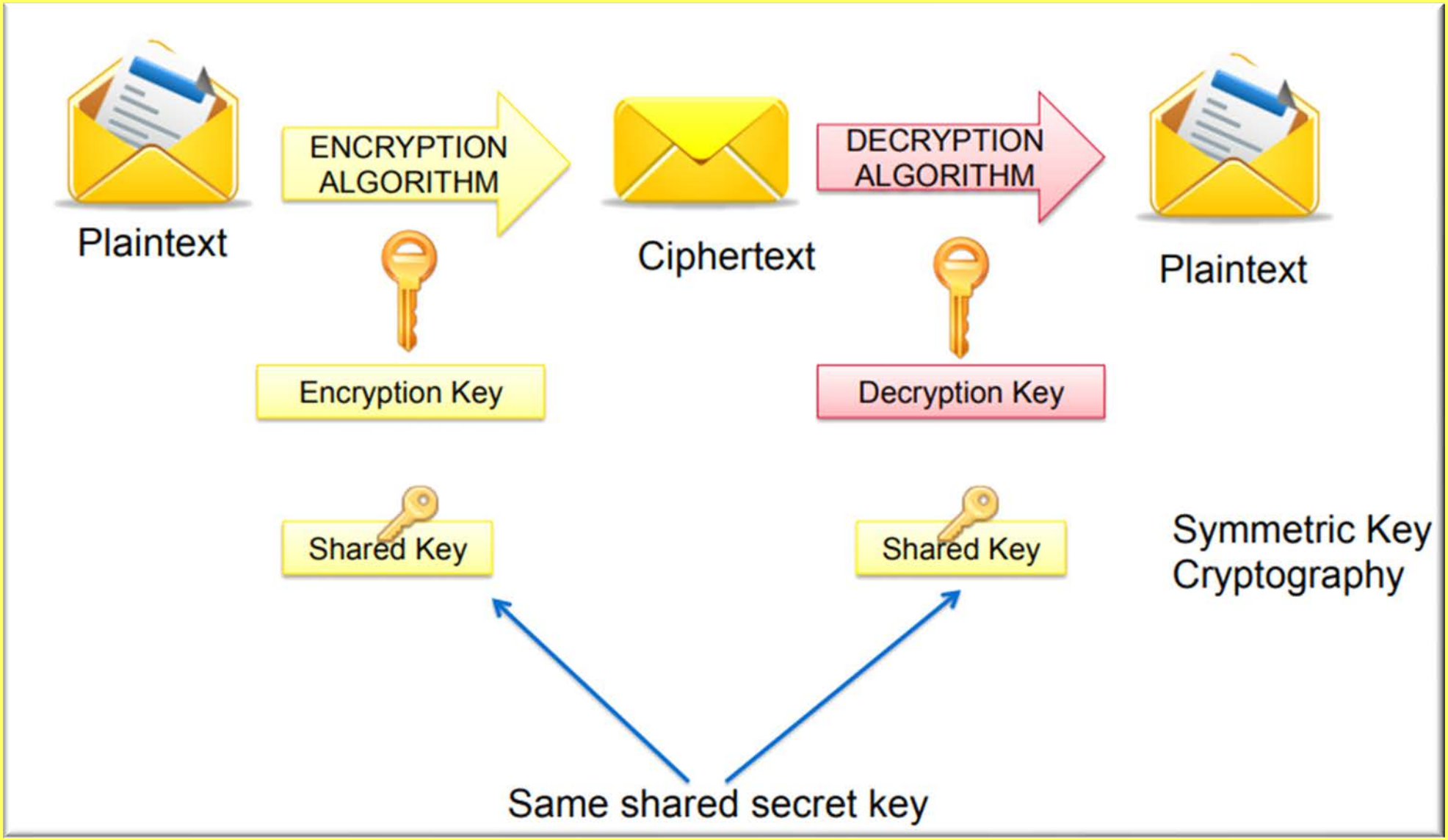
ONE-TIME PADS: A PERFECT SUBSTITUTION

- There is one type of substitution cipher that is **absolutely unbreakable**.
  - The one-time pad was invented in 1917 by Joseph Mauborgne and Gilbert Vernam and is also known as Vernam cipher
  - We use a block of shift keys, (k_1, k_2, . . . , k_n), to encrypt a plaintext, M, of length n, with each shift key being chosen uniformly at random.
- Since each shift is random, every ciphertext is equally likely for any plaintext.
- In spite of their perfect security, one-time pads have some weaknesses
- The key has to be as long as the plaintext
- Keys can never be reused
  - Repeated use of one-time pads allowed the U.S. to break some of the communications of Soviet spies during the Cold War
- Such cipher is **difficult to break but not very practical**

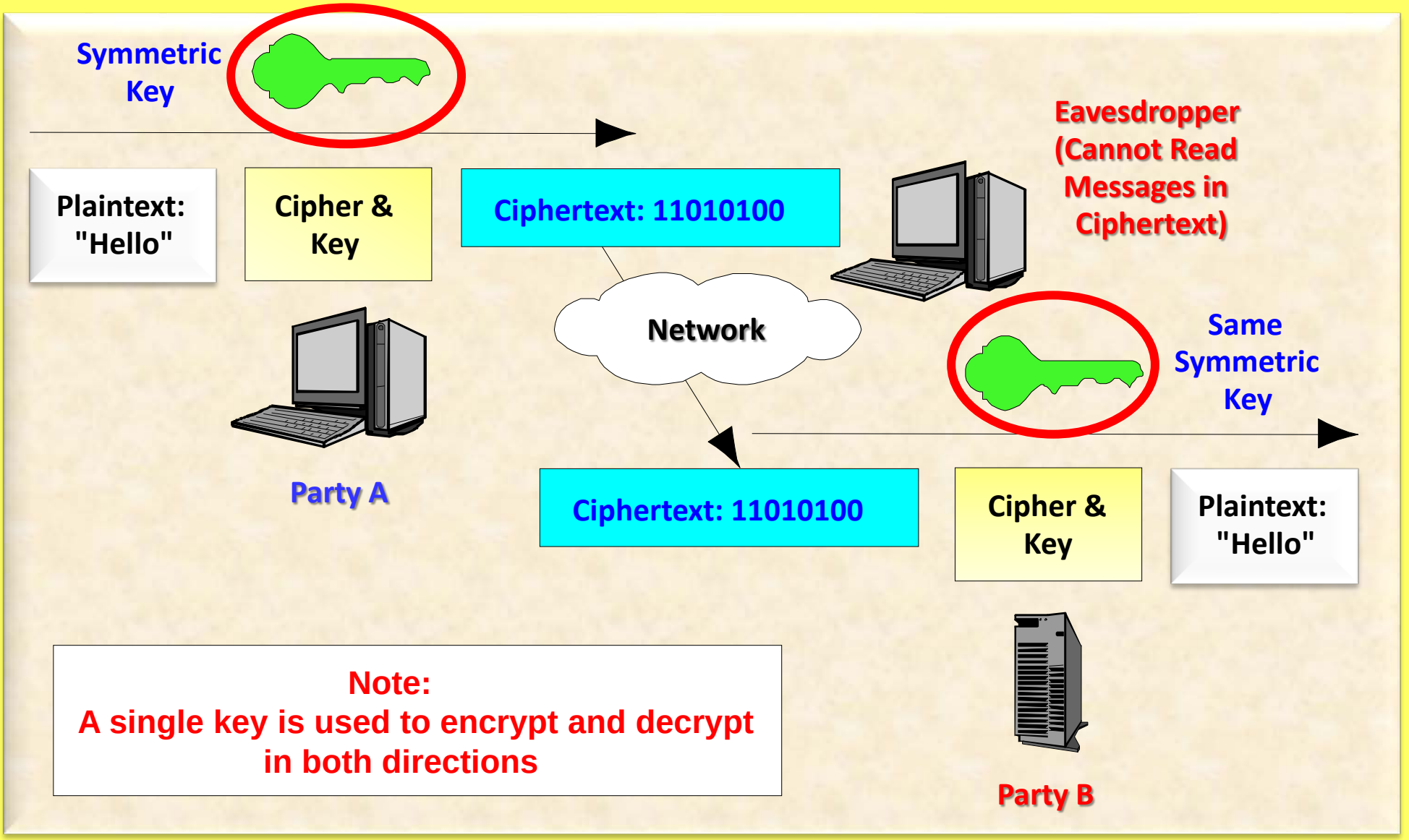
MODERN CIPHERS

- Operate on binary plaintext
- Uses binary keys of fixed length
- Different types of ciphers:
  - Symmetric ciphers
    - Stream ciphers (RC4, A5/x, Helix, SEAL)
    - Block ciphers (DES, Triple-DES, Blowfish, AES)
  - Asymmetric ciphers
    - Diffie-Hellman, ElGamal, RSA, ECC
- Two basic operations in modern cipher are:
  - Substitution: Substitutes a code symbol for another.
    - Example: shifts (Vigenere cipher), xor
  - Permutation: Transposes or re-orders the symbols present in the code
- Both steps are needed for security

SYMMETRIC KEY ENCRYPTION



SYMMETRIC KEY ENCRYPTION FOR CONFIDENTIALITY



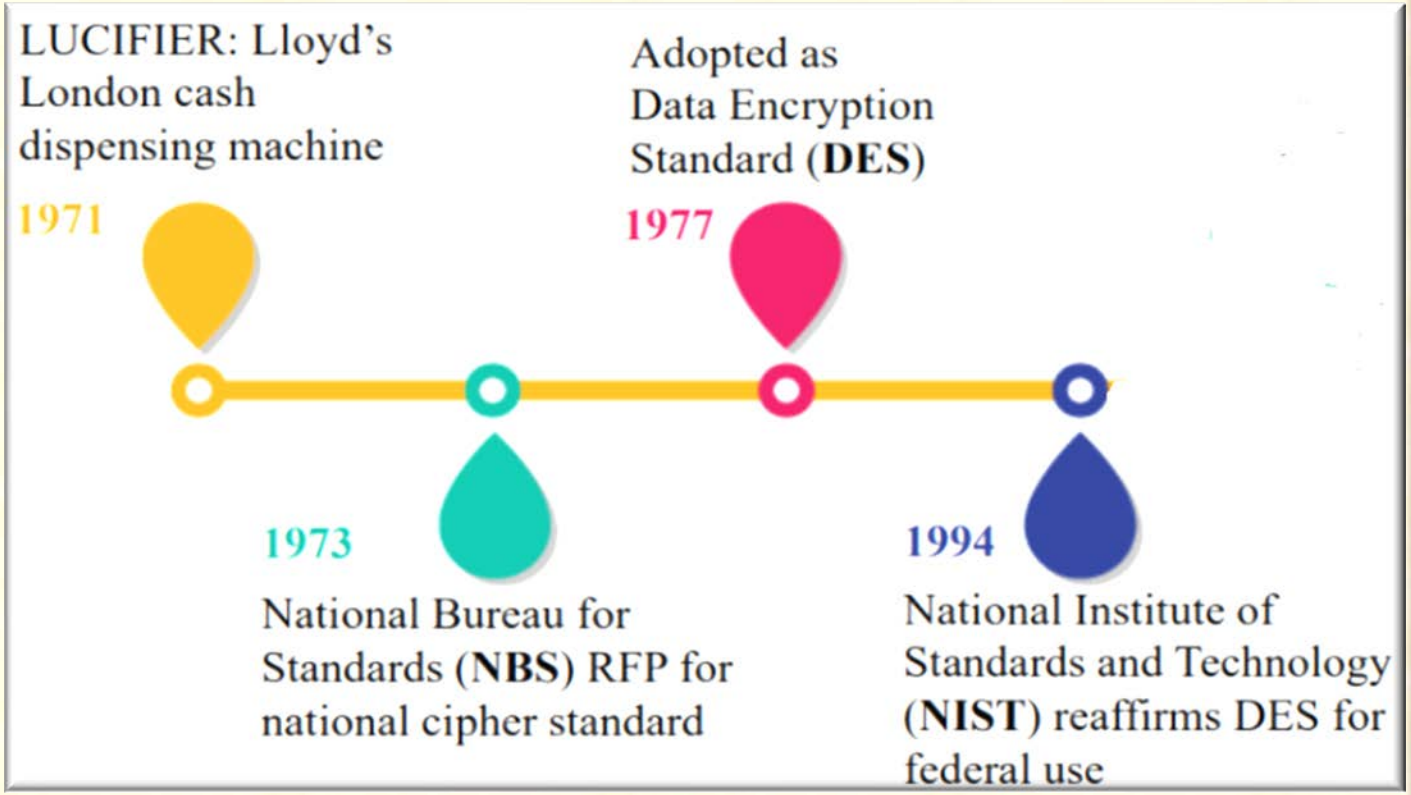
Note:
A single key is used to encrypt and decrypt in both directions

SECRET-KEY CRYPTOGRAPHY (SKC)

- **ADVANTAGES OF SKC**
  - Symmetric-key ciphers can be designed to have high rates of data throughput.
  - Some hardware and software implementations achieve encrypt rates of hundreds of megabytes per second.
  - Keys for symmetric-key ciphers are relatively short.
    - For example, 128-bit keys are considered very safe.
- **DISADVANTAGES OF SKC**
  - In a two-party communication, the key must remain secret at both ends.
  - In a large network, there are many key pairs to be managed. Consequently, effective key management requires the use of an trusted third-party (TTP).
- **POPULAR SYMMETRIC ENCRYPTION ALGORITHMS**
  - **DES, 3DES, AES**, CAST, RIVEST, Blowfish, IDEA

DATA ENCRYPTION STANDARD (DES)

- In 1973, the National Bureau of Standards (NBS) now National Institute of Standards and Technology (NIST) requested proposals for national symmetric-key cryptosystem.
- A proposal from IBM, a modification of a project called Lucifer, was accepted as DES and adopted in 1976-77.

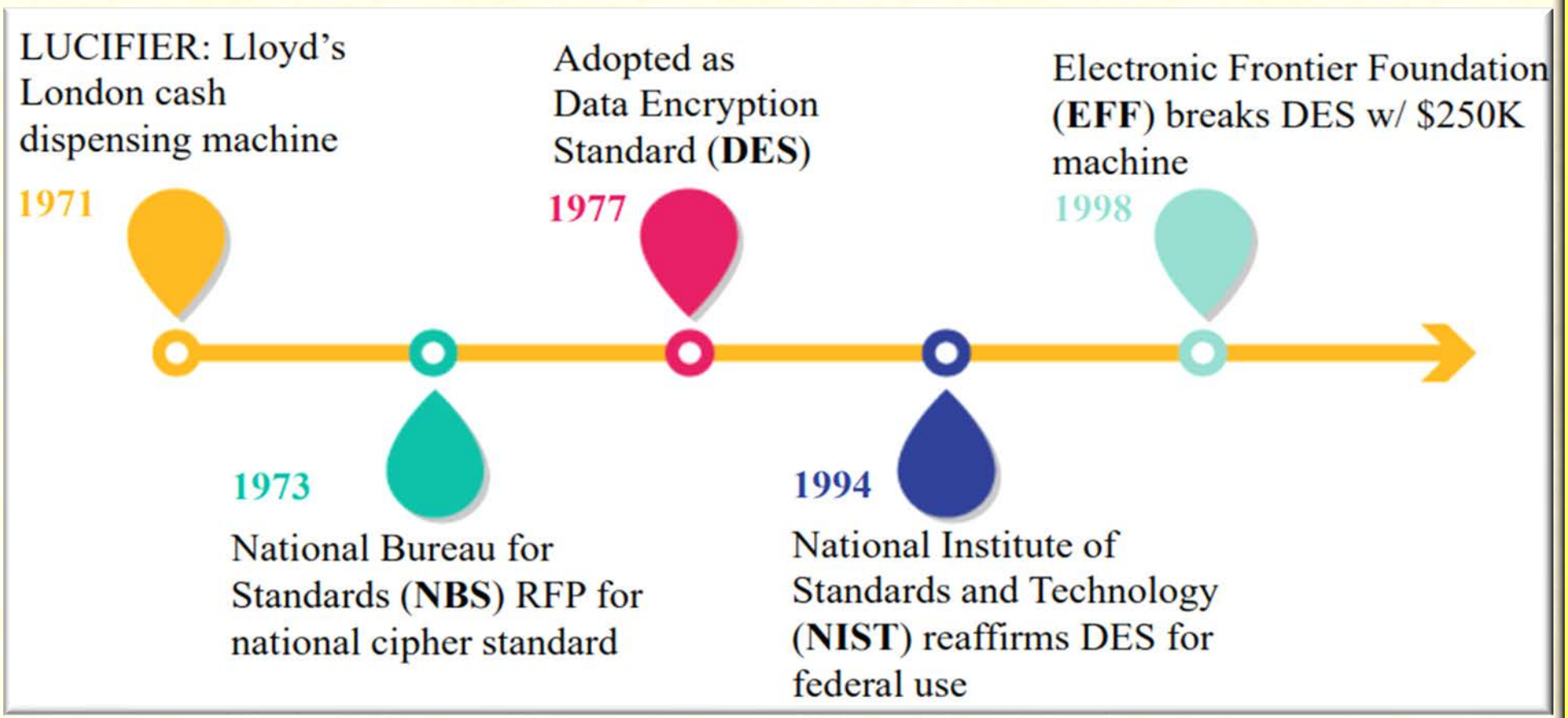


DATA ENCRYPTION STANDARD (DES)

- DES once was the most popular symmetric encryption cryptosystems.
- It was the first crypto system to have been used in commercial applications.
- It is a block cipher with 64-bit block size and 56-bit key.
- The algorithm takes the plain text in 64-bit blocks and converts them into 64-bit blocks of ciphertext using 56-bit keys.
- Since it's a symmetric-key algorithm, it employs the same key in both encrypting and decrypting the data.
- DES was adopted by NIST in 1976 as federal standard for encrypting non-classified information.
- After becoming the approved federal encryption standard in November 1976, it was subsequently reaffirmed as the standard in 1983, 1988, and 1999.
- The NIST had to replace the DES algorithm because its 56-bit key lengths were too small, considering the increased processing power of newer computers.
- DES's dominance came to an end in 2002 and the NIST officially withdrew the 1999 reaffirmation in May 2005.

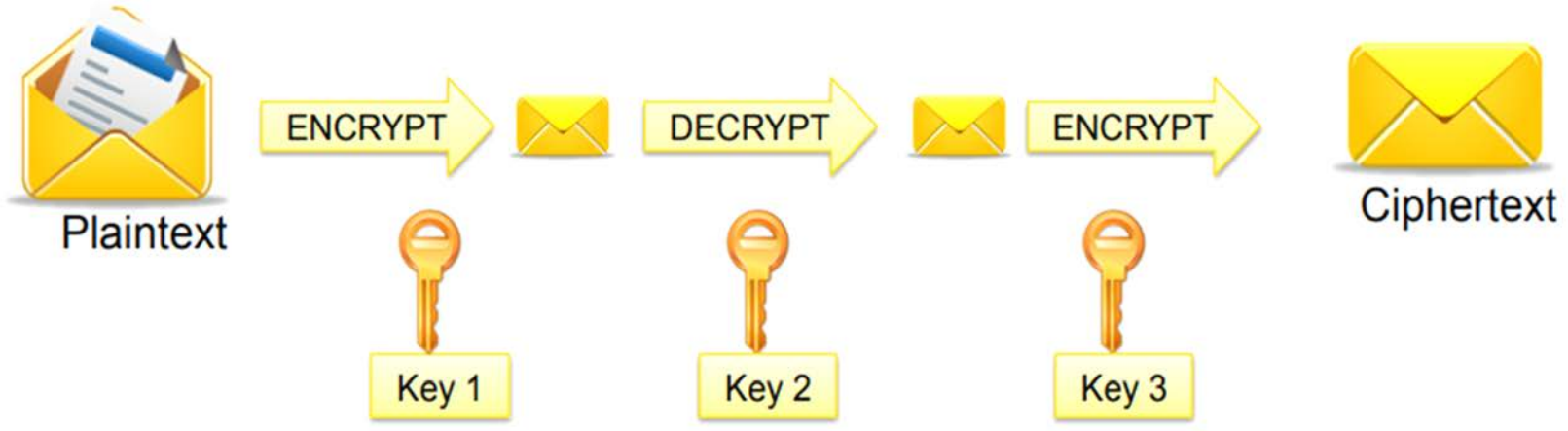
SOMEONE BROKE DES, SO WHAT?

- Use DES multiple times?
- How many Times?



3DES

- Triple DES is a symmetric key-block cipher which applies the DES cipher in triplicate. It encrypts with the first key (k1), decrypts using the second key (k2), then encrypts with the third key (k3). There is also a two-key variant, where k1 and k3 are the same keys.



- Note:
  - If Key1 = Key2 = Key3, this is similar to DES
  - Usually, Key1 = Key3

AES (ADVANCED ENCRYPTION STANDARD)

- Originally called Rijndael, the cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen.
- It is block size is 128 and key size varies according to the version.
- Three versions are known as AES-128, AES-192 and AES-256, respectively.
- Although no efficient attacks exist against AES, in 2011, the trio of CRYPTOGRAPHY RESEARCHERS (working at Microsoft and European Universities) identified a weakness in AES security algorithm that can crack secret keys faster than before.
- However, recovering a key is no five-minute job and despite being four times easier than other methods the number of steps required to crack AES-128 is an 8 followed by 37 zeroes.

Vincent Rijmen
born in 1970

Joan Daemen
born in 1965

PUBLIC (ASYMMETRIC) KEY CRYPTOGRAPHY

- SYMMETRIC ALGORITHMS ARE **IMPORTANT BECAUSE**
  - They are comparatively fast and have few computational requirements
- THEIR **MAIN WEAKNESSES**
  - Two geographically distant parties both need to have a key that matches the other key exactly.
  - Secure key exchange can be an issue.
- Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations, which wanted to securely store the classified communication.
- However, the symmetric key was found to be non-practical when two parties want to securely communicate. This gave rise to public cryptosystem.
- **PUBLIC KEY** (ALSO KNOWN AS ASYMMETRIC-KEY ENCRYPTION)
  - Uses two different but related keys
  - Either key can encrypt or decrypt message
  - If Key A encrypts message, only Key B can decrypt
  - One key serves as private key and the other serves as public

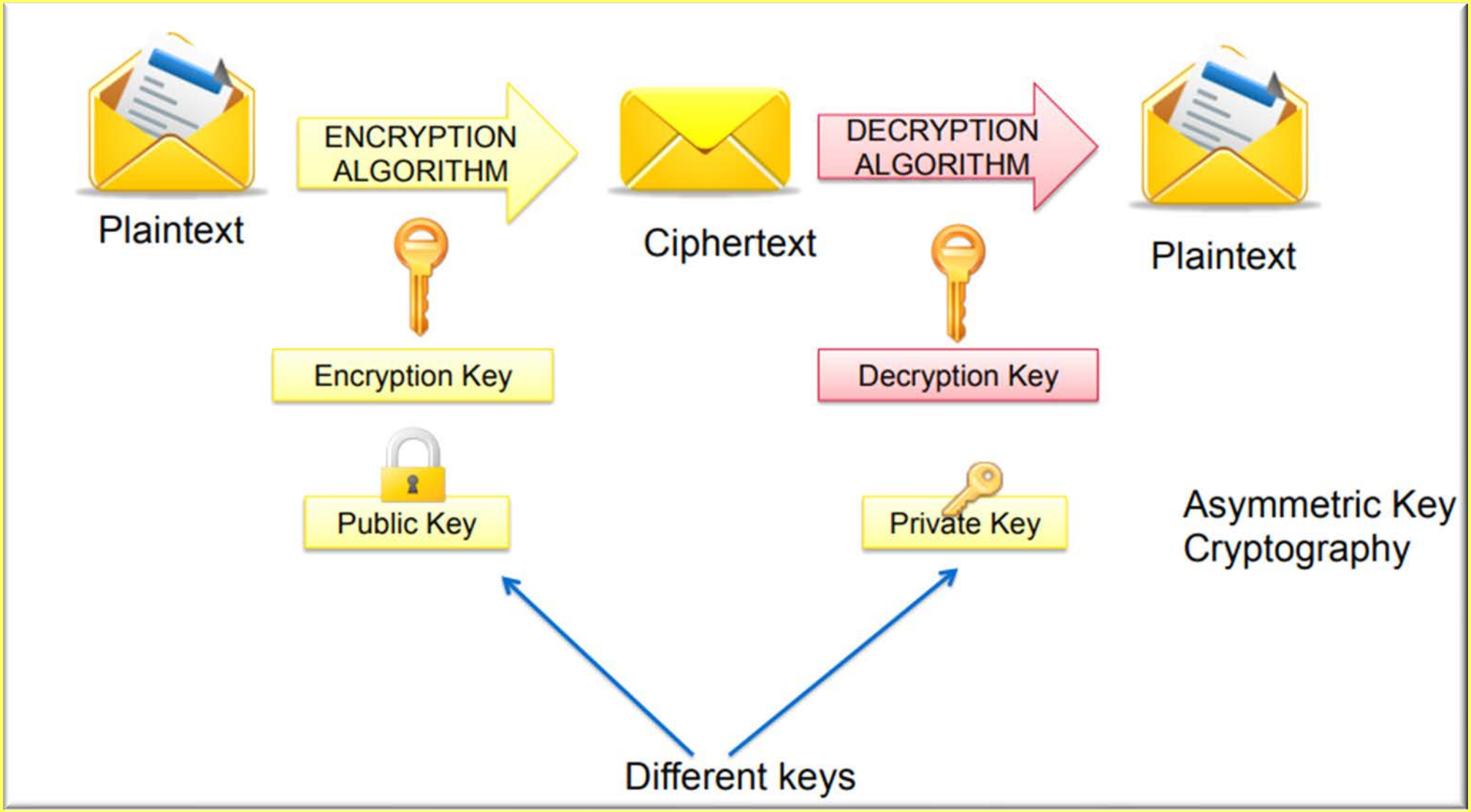
PUBLIC-KEY CRYPTOGRAPHY (PKC)

- PKC was invented by Whitfield **Diffie** and Martin **Hellman** in 1976
  - PhD students at Stanford University

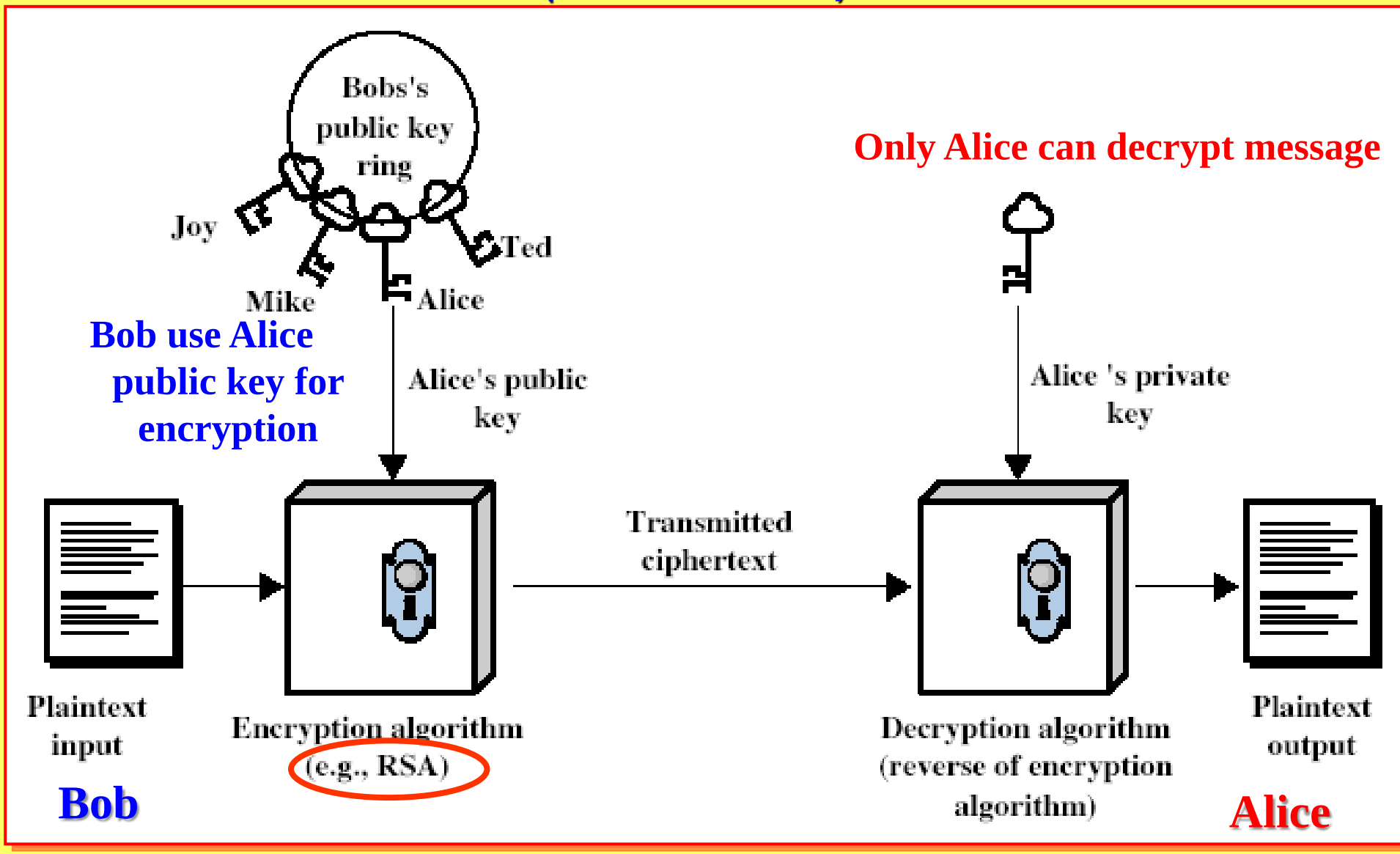

- Some give credit to Ralph Merkle (in 2002, he was recognized)

- NSA says that they knew PKC back in 60's
  - Uses two different but related keys
  - Either key can encrypt or decrypt message
  - If Key A encrypts message, only matching Key B can decrypt
  - One key serves as private key and the other serves as public key
- **PUBLIC KEY ALGORITHMS**
  - DIFFIE-HELLMAN, El-Gamal, RSA and Elliptic Curve (**used in Bitcoin)**

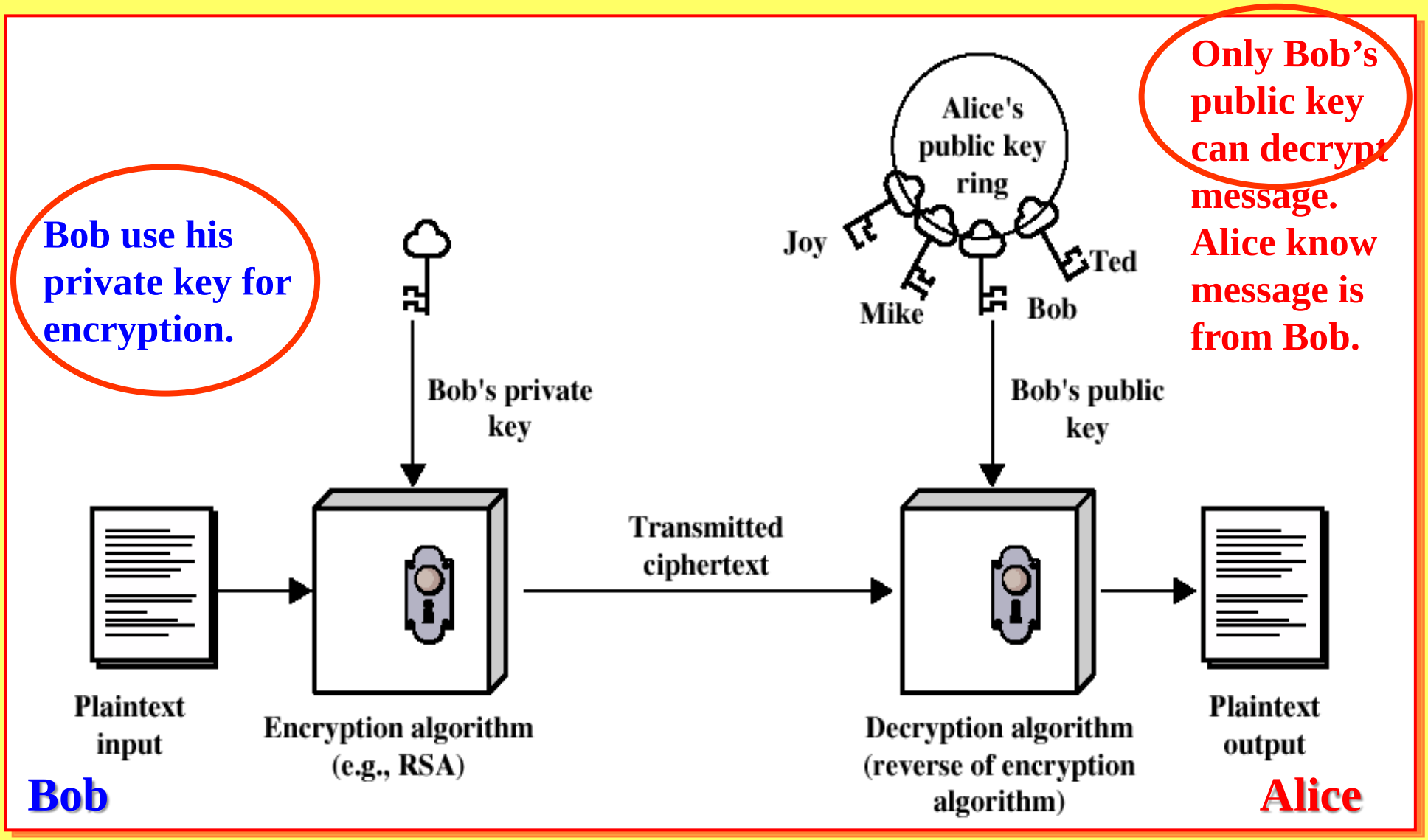
PUBLIC-KEY CRYPTOGRAPHY (PKC)



PUBLIC KEY ENCRYPTION
(CONFIDENTIALITY)



PUBLIC KEY AUTHENTICATION



PRIME NUMBERS AND MOD

- **PRIME NUMBERS**
- Prime numbers only have divisors of 1 and self
  - they cannot be written as a product of other numbers
  - note: 1 is prime, but is generally not of interest
- eg. 2,3,5,7 are prime, 4,6,8,9,10 are not.
- **MOD:** Example 1: 15 mod 20
  - Since 15 < 20, answer = 15 (i.e. 15 is remainder)
- **Example 2: 320 MOD 9**
  - Use MOD key on the calculator

  - If your calculator doesn't have MOD key, you can use division
  - 320/**9** = **3 5** . **5 5 5 5 5**
  - Now take the value after decimal point, which is **0.5555** and **multiply** it with **9**
  - **0.5555 * 9** = **5** This is the MOD value

PUBLIC KEY ALGORITHMS

RSA CRYPTOSYSTEM

- This cryptosystem is one the first which provided complete solution.
  - How to generate public and private key
  - How to encrypt and decrypt the data
  - How to generate and verify digital signature
- It remains the most employed cryptosystem even today.
- The system was invented by three scholars Ron Rivest, Adi Shamir, and Len Adleman and hence, it is termed as RSA cryptosystem in 1978.
- The security of RSA algorithm is based on factorizing large prime numbers.
- The fact that it is easy to calculate the product of two numbers, while it is extremely difficult (if not impossible) to find the factor of two numbers, when the size is extremely large.
- This is called one way function, which means easy to compute but it is very difficult to compute their inverse functions, unless you know the secrete (private key).

PUBLIC KEY ALGORITHMS

- **ELGAMAL**
- It was designed by Taher Elgamal in 1985
  - Based on original ideas of Diffie and Hellman
  - Security based on assumed difficulty of discrete log
  - Consists of both encryption and signature algorithms
  - Cipher text is twice the size of plain text
  - It is slow
- **ELLIPTIC CURVE CRYPTOGRAPHY (ECC)**
  - In 1985, Neal Koblitz and Victor Miller - proposed using elliptic curves, however it only saw wide use in 2005
  - Majority of public-key crypto (RSA, D-H) uses large numbers and imposes a significant load in storing and processing keys and messages
  - ECC on the other hand uses elliptic curves and offers same security with smaller bit sizes
  - Even though RSA is still widely used, in recent times, ECC is becoming very popular, particularly after its use in crypto currencies

PUBLIC KEY + SYMMETRIC

- **PROBLEM**: Public key systems are powerful but slow, while symmetric systems are inflexible but fast.
- **SOLUTION**: A hybrid system!
  - Sender generates random symmetric session key
  - Sender encrypts session key using receivers' public key
  - Receiver decrypts it using his/her private key and now both have the shared session key
- **RESULT**: A fast, flexible system
- **HYBRID SCHEME**
- Combine advantages of symmetric and asymmetric ciphers
  - Throughput of symmetric cipher
  - Key management of asymmetric cipher
- A two-stage approach is used
  - In the first step public key cryptography is used to derive a session key.
  - Subsequently, the session key is used to encrypt the actual message.

HYBRID SYSTEM

Client

Server

Client request a session

Digital certificate, Public and private Key

Digital certificate and public key sent back

Encrypted session key (#$%^) sent to server

1. Client create session key (Symmetric key) e.g 3486
2. Session Key encrypted with the Server's public key (#$%^)

Session key decrypted with private Key (3486)

Session encrypted with symmetric session key

DIGITAL SIGNATURES

- A digital signature ("digital thumbprint") is a message digest used to cryptographically sign a message.
- Digital signatures rely on asymmetric (public key) cryptography.
- To create a digital signature, you sign the message with your private key. The digital signature then becomes part of the message.
- This has two effects:
  - Any changes to the message can be detected, due to the message digest algorithm.
  - You can not deny signing the message, because it was signed with your private key.
- These two features, message integrity and non-repudiation, make digital signatures a very useful component for e-commerce applications.
- Digital signature can be used in all electronic communications
- It is an electronic stamp or seal that is append to the document.
- Ensure that the document remains unchanged during the transmission

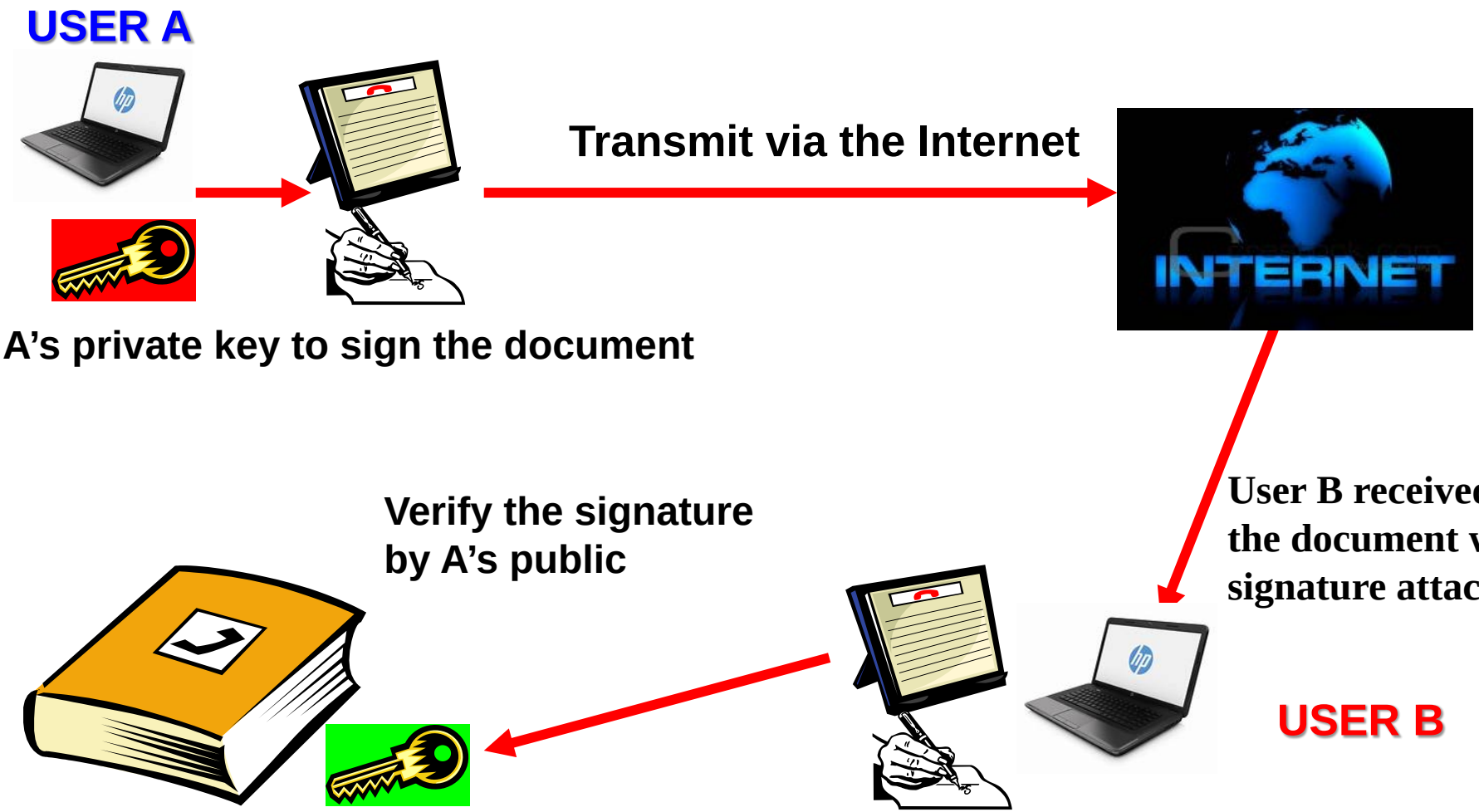
KEY SIZE

- When deploying ciphers, the size of key is very important.
- The strength of many encryption applications and cryptosystems is measured by key size.
- For cryptosystems, the security of encrypted data is not dependent on keeping the encrypting algorithm secret.
- Cryptosystem security depends on keeping some or all of elements of key secret.
- **There are two keys**
- Private and Public key: These keys are used to exchange the symmetric key. For RSA algorithms, a key size of 2048 (2K) is considered safe.
- **Session key**: This is secret key (symmetric key), which is used during the communication between client and server. A key size of 128 or more is considered very reasonable. A key size of 256 is considered very safe and secure, however it will be slower than the algorithm with key size of 128. The key size also depend on the actual algorithm, as some algorithms use fixed key size, while others like AES, has different versions for different key sizes.

PROPERTIES OF DIGITAL SIGNATURES

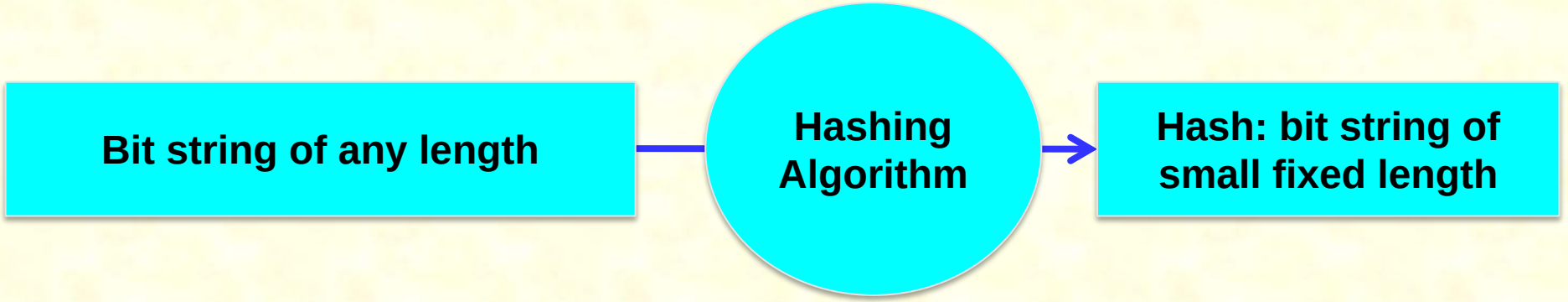
- Only private-key holder can compute signatures.
- Any holder of matching public-key can verify signature.
- Digital signature schemes work with two major steps:
  - Prepare a message representative
  - Apply a signature transform.
- The general verifying method is generally similar to the signing method
  - Undo the signature transformation
  - Check the message digest for any issues
- **HOW DOES DIGITAL SIGNING WORK?**
- We extract a value (binary string) from the message with a hash function.
- We use a digital signature algorithm to produce the signature from the hash value and the private key.
- The message can now be authenticated with the public key and the signature

HOW DIGITAL SIGNATURE WORKS?



DIGITAL SIGNATURE

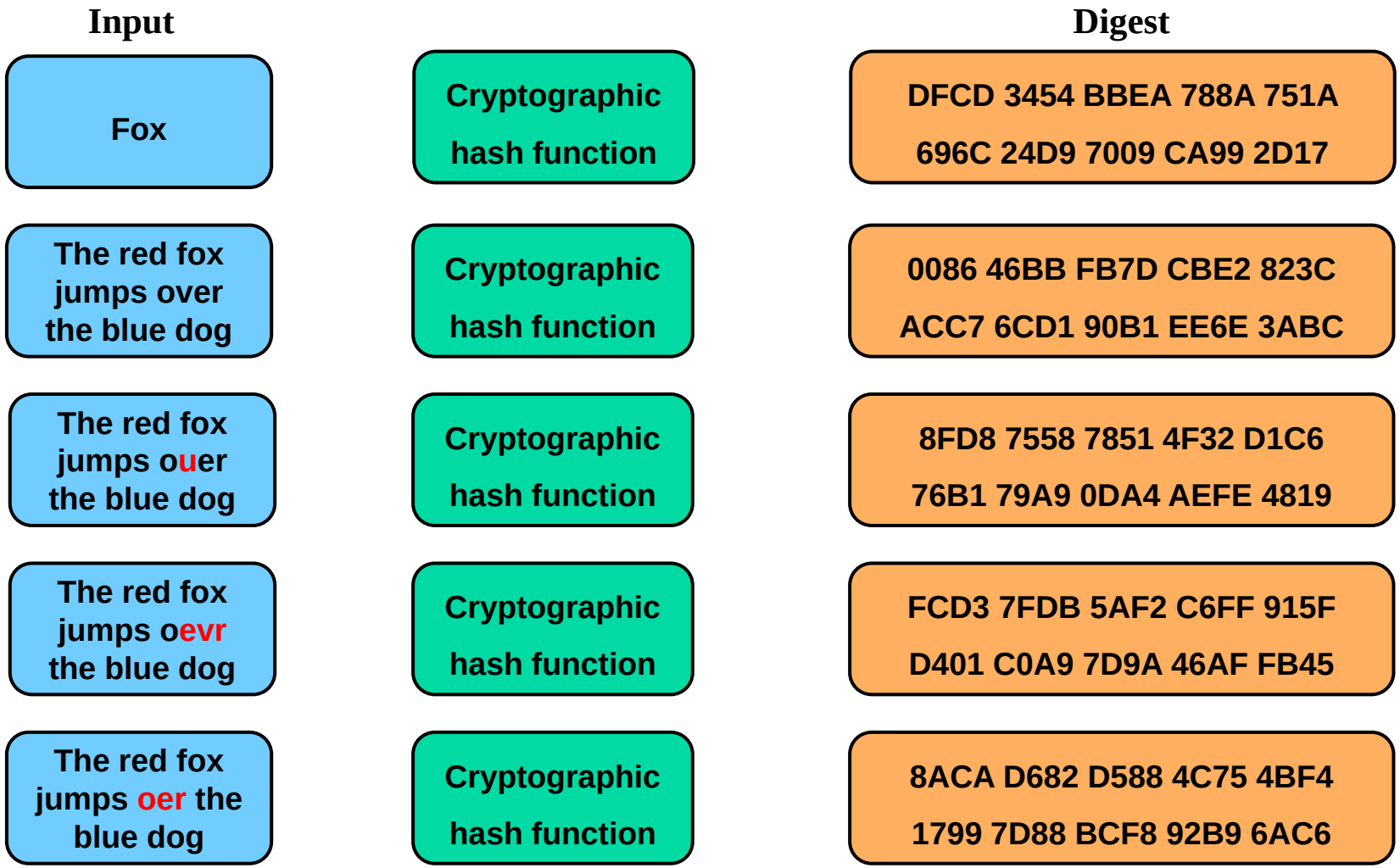
- **DIGITAL SIGNATURE SCHEME:** Two components
  - A private signing algorithm which permits a user to securely sign a message
  - A public verification algorithm which permits anyone to verify that the signature is authentic.
- **HASHING**
- A hashing algorithm is applied to a bit string of any length
- It is designed in such a way that every bit in the message has some effect on the resulting message digest.
- The message digest can then be input to the Digital Signature Algorithm (DSA) which generates or verifies the signature for the message



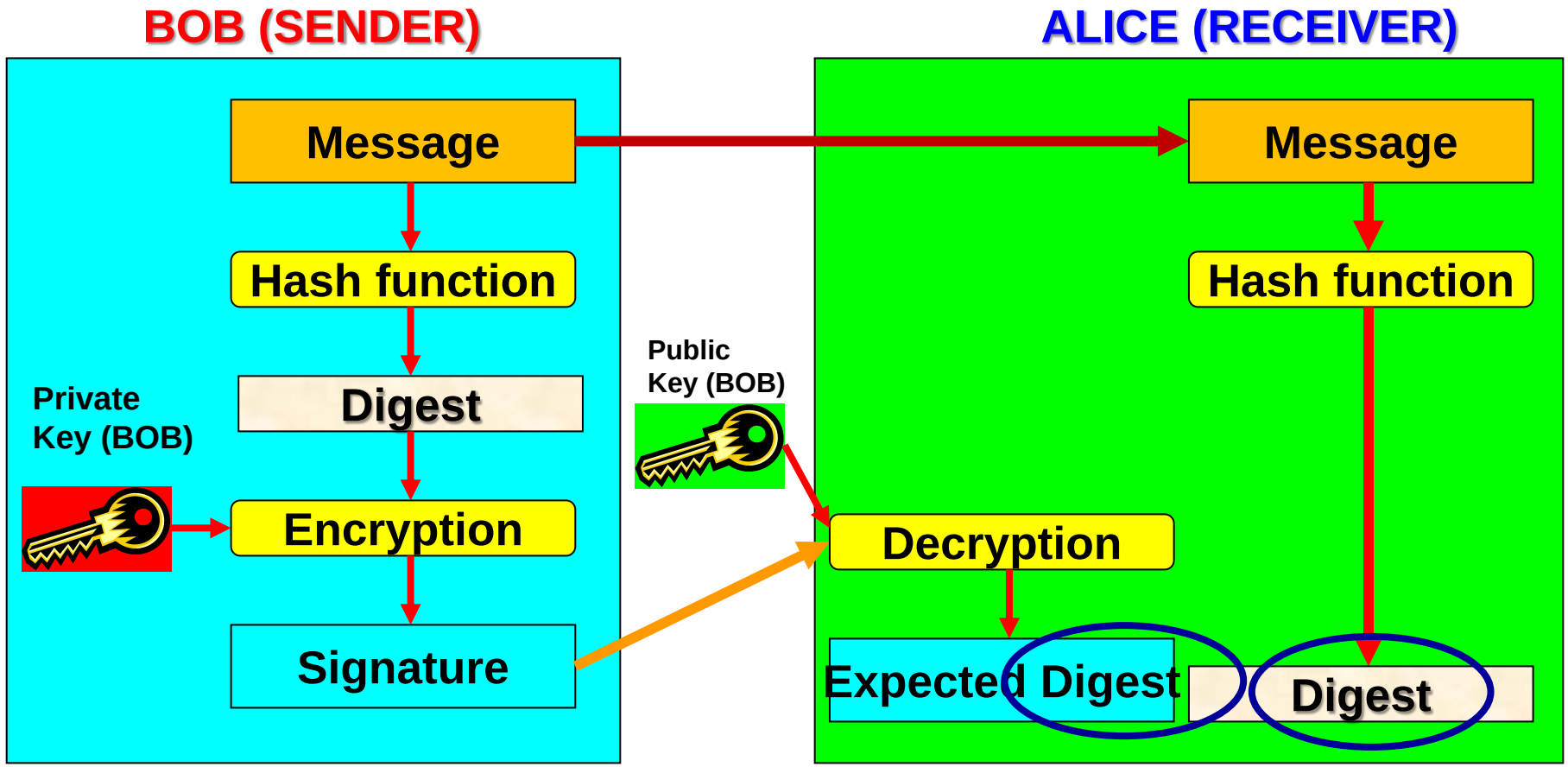
HASH FUNCTION PROPERTIES

- Can be applied to a block of data of any size
- Produces a fixed-length output
- H(x) is relatively easy to compute for any given x
- One-way or pre-image resistant
  - Computationally infeasible to find x such that H(x) = h
- Computationally infeasible to find y ≠ x such that H(y) = H(x)
- Collision resistant or strong collision resistance
  - Computationally infeasible to find any pair (x,y) such that H(x) = H(y)

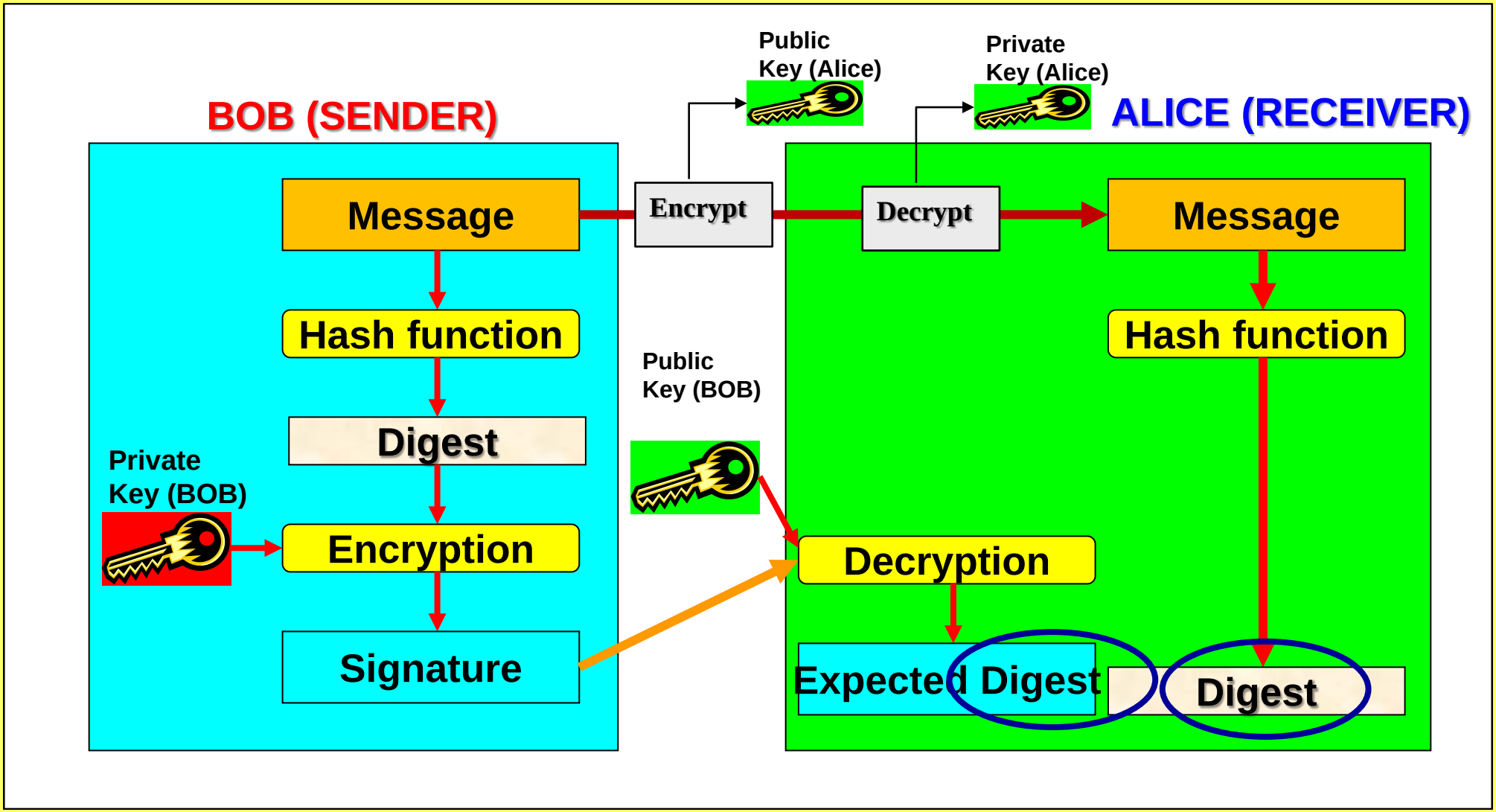
Note that even small changes in the source input (here in the word "over") drastically change the resulting output.



DIGITAL SIGNATURE
(WITHOUT MESSAGE PROTECTION)

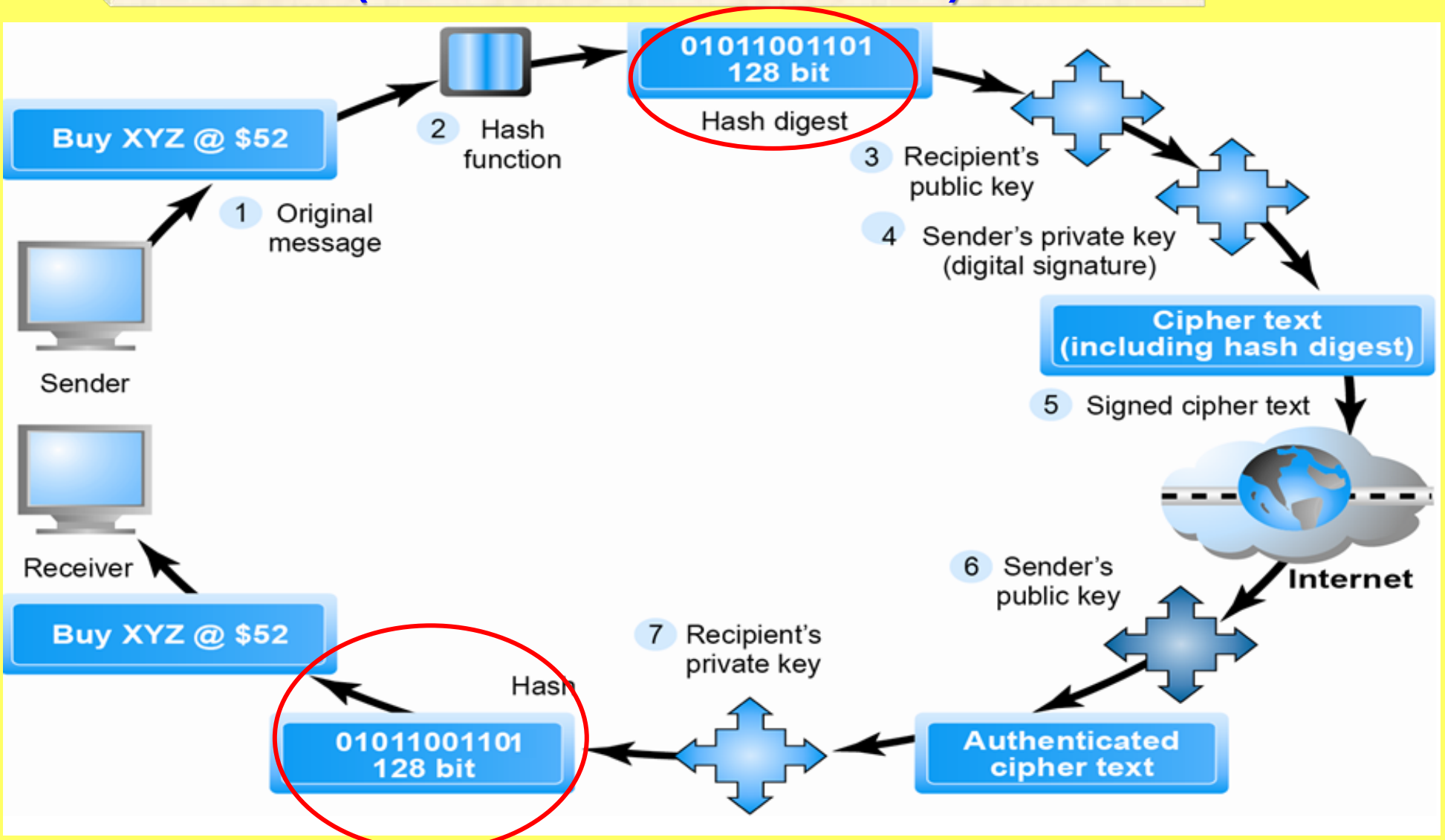


DIGITAL SIGNATURE
(WITH MESSAGE PROTECTION)



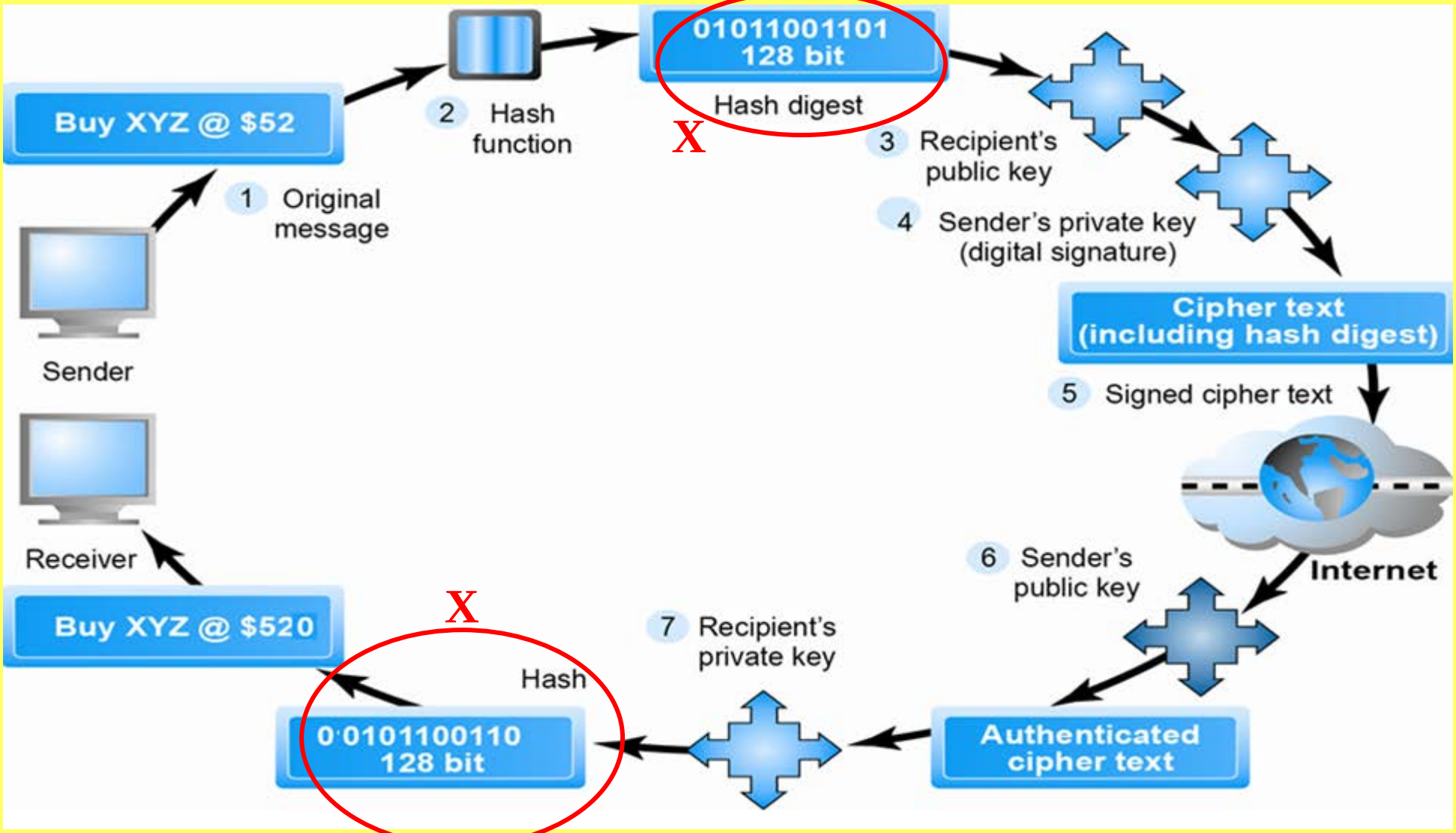
DIGITAL SIGNATURE EXAMPLE 1

(WITH MESSAGE PROTECTION)



DIGITAL SIGNATURE EXAMPLE 2

(WITH MESSAGE PROTECTION)



DIGITAL CERTIFICATES & CERTIFICATE AUTHORITIES

- A digital certificate is an electronic document, similar to a digital signature, attached to a file certifying that this file is from the organization it claims to be and has not been modified from the original format
- A Certificate Authority is an agency that manages the issuance of certificates and serves as the electronic notary public to verify their worth and integrity
- For digital signatures to work, a trusted third party known as a Certification Authority (CA) is needed to issue digital certificates that certify the electronic identities of users and organisations.
- Some Trusted CA operating in Singapore
  - Verisign
  - GlobalSign
  - **Netrust Pte Ltd**

DIGITAL CERTIFICATE

- **Digital certificate includes:**
  - Name of subject/company
  - Subject's public key
  - Digital certificate serial number
  - Expiration date, issuance date
  - Digital signature of CA

I hereby certify that the public key
19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A
belongs to
Robert John Smith
12345 University Avenue
Berkeley, CA 94702
Birthday: July 4, 1958
Email: bob@superdupernet.com

SHA-1 hash of the above certificate signed with the CA's private key

1. Generate Key-pair

2. User-A requests CA Certificate

3. CA responds with its CA Certificate including its Public Key

4. Gather information

5. Request the Certificate which has User-A's identity and Public Key

6. CA verifies the identity of User-A

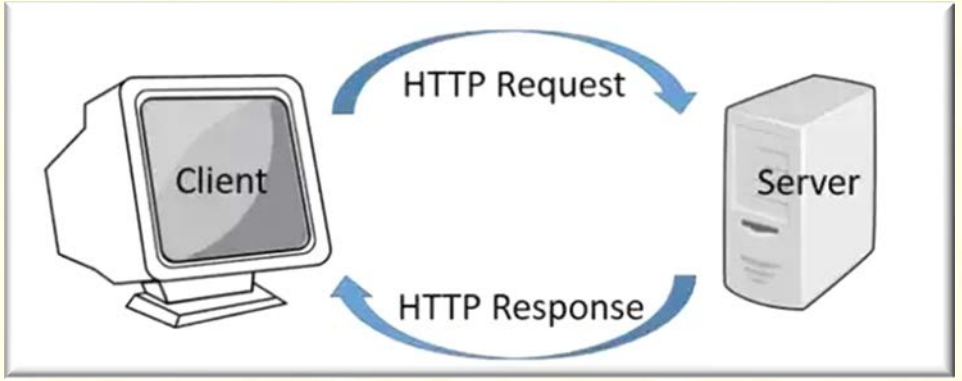
7. Issue the Certificate for User-A

Public-Key Infrastructure (PKI)

- Integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services enabling users to communicate securely
- PKI systems are based on public-key cryptosystems
- PKI protects information assets in several ways:
  - Authentication
  - Integrity
  - Privacy
  - Authorization
  - Nonrepudiation
- Typical PKI solution protects the transmission and reception of secure information by integrating:
  - A certificate authority (CA)
  - A registration authority (RA)
  - Certificate directories
  - Management protocols
  - Policies and procedures

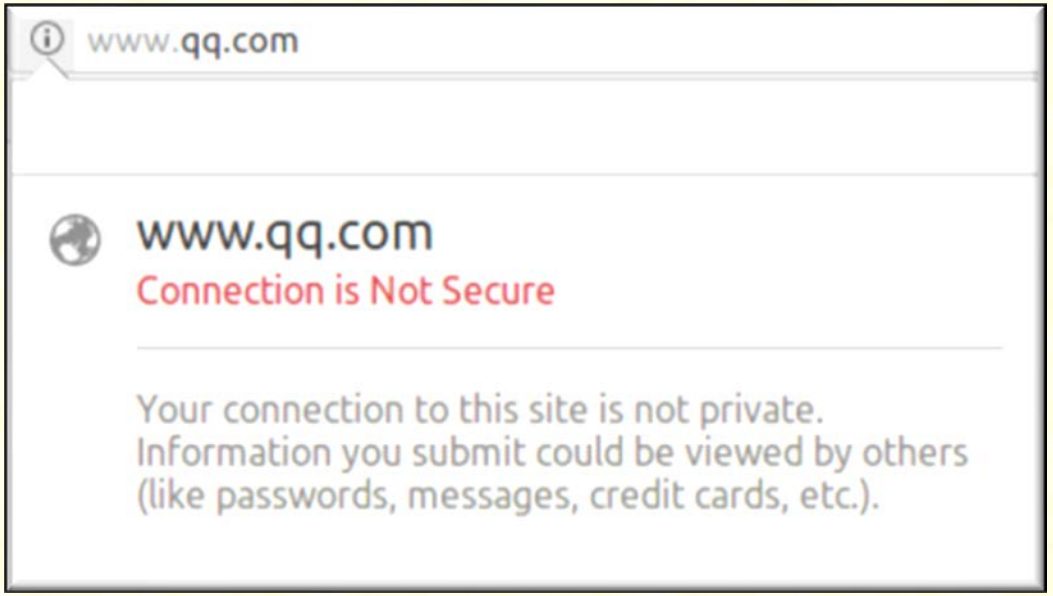
WEB SECURITY

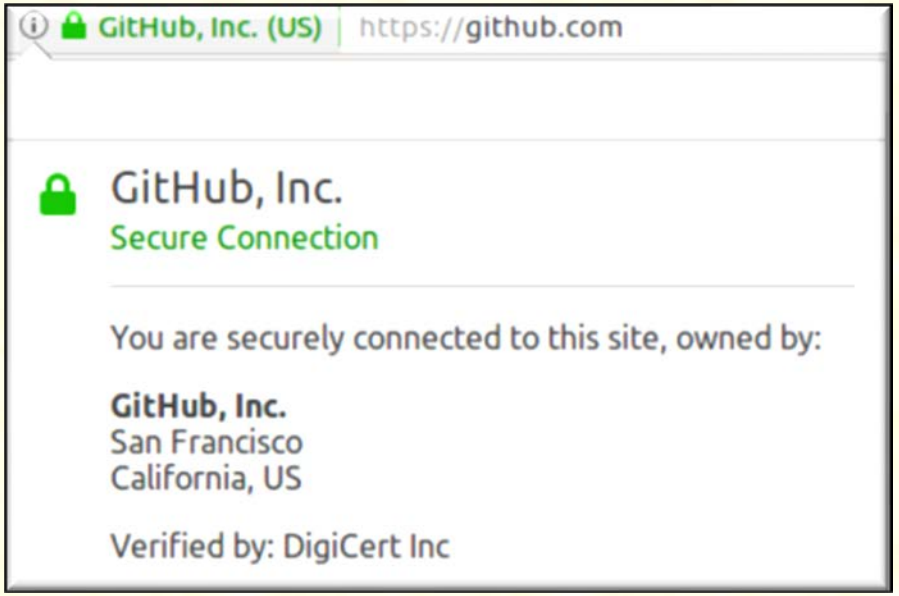
- Web is widely used by business, government and individuals. However, Internet & Web are vulnerable as it uses HTTP protocol.
- **HTTP IS NOT A SECURE PROTOCOL**
  - It is a simple and stateless client/server application running over TCP/IP.
- **WHAT ARE THE THREATS**
  - **INTEGRITY**
    - Data modification, insertion
  - **CONFIDENTIALITY**
    - Eavesdropping on the net
    - Theft from server machine
  - **AUTHENTICATION**
    - Impersonation, data forgery
  - **DENIAL OF SERVICE**
    - Hacked web servers



WEB SECURITY

- **ADDED SECURITY MEASURES NEEDED**
  - The SSL (Secure Socket Layer, originated by Netscape) and TLS (Transport Layer Security) was designed for web security. First version of TLS can be viewed as an SSLv3.1
- **HTTPS**
  - Secure HTTP protocol = HTTP+ SSL





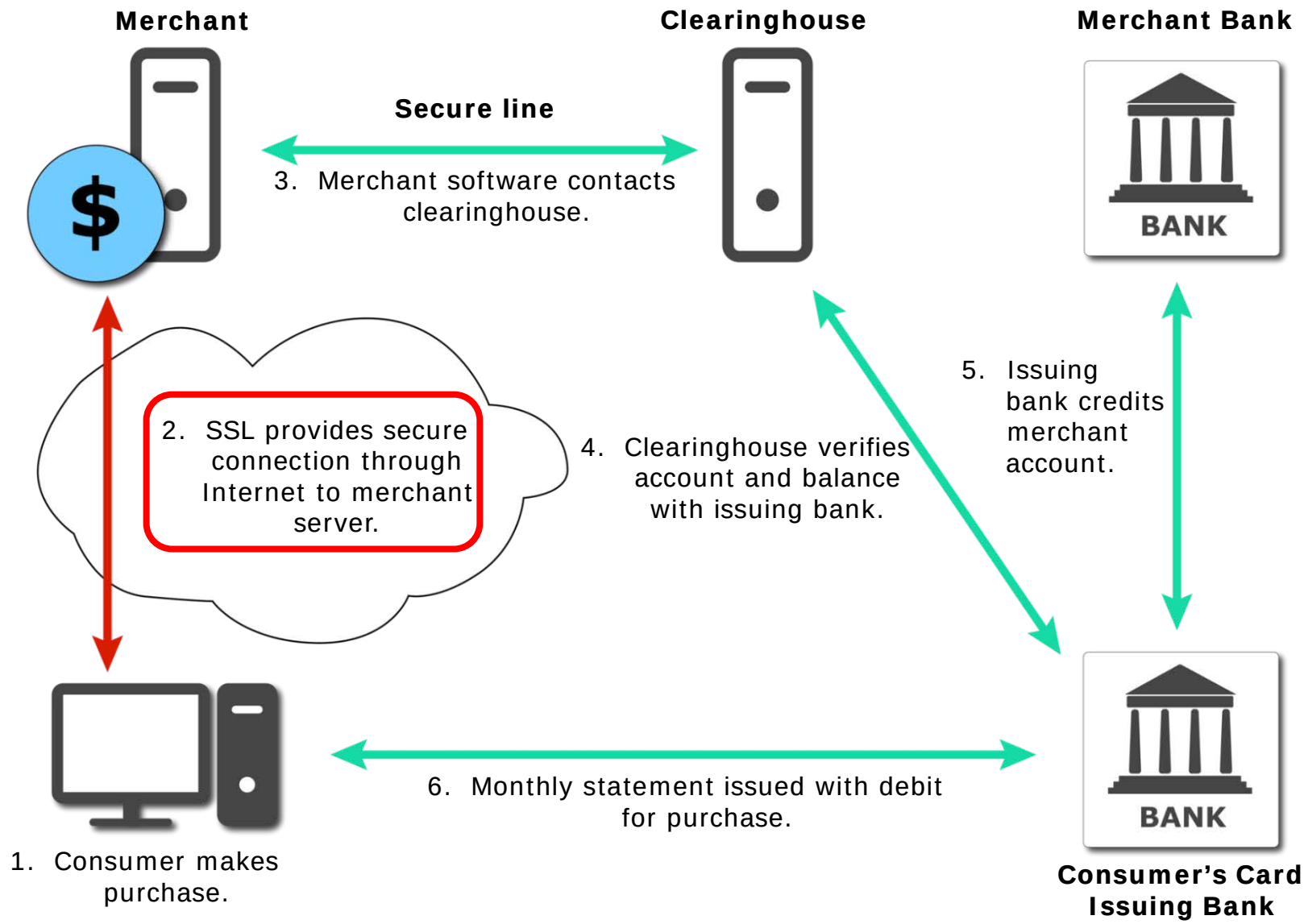
SSL (SECURE SOCKET LAYER)

- Can provide server authentication with digital certificate (X509).
- It can authenticate client (rare).
- Can provide privacy by encryption.
- Can be used with any TCP app (**but mainly http, email**).
- **HISTORY**
  - Internal Netscape design, early 1994.
  - SSLv1 was broken by members of audience while it was being presented.
  - SSLv2 was shipped with Navigator 1.0, in November 1994, however it was vulnerable to man-in-the-middle attack.
  - SSLv3 was designed by **Netscape and Paul Kocher**, in November 1996 and was designed with public input/feedback.
  - SSL is easy to apply and use because it is built in all major Web browsers (IE, Opera, Chrome, Mozilla, Firefox) and servers.

TRANSPORT LAYER SECURITY (TLS)

- By the end of the 1990s, Netscape handed SSL over to the IETF(Internet Engineering Task Force).
- The (IETF), renamed SSL 3 as Transport Layer Security (TLS) in 1999 and made SSL obsolete in 2015.
  - SSL version 3.0 was adopted by Internet Engineering Task Force (IETF) as TLS version 1.0.
  - All TLS versions up to 1.2 were backward-compatible with SSL 3.0, however, backward compatibility with SSL was removed from TLS 1.3.
  - The latest version: TLS1.3 (Finalized on March 21st, 2018).
  - Many people still refer to web encryption as SSL, even though the vast majority of services have switched over to supporting TLS only.

ONLINE CREDIT CARD TRANSACTION (SSL)



ISSUES WITH SSL/TLS

- It slows down servers.
- It protects data in transit, but not databases.
- SSL/TLS **Cannot:**
  - Authenticate the actual operator of a computer
  - Authenticate the owner of an online shop (merchant)
  - Authenticate the actual online consumer
  - Authenticate other parties involved in online payment system
  - Protect the use of stolen credit cards online

Securing Wireless Networks with WEP and WPA

- Wired Equivalent Privacy (WEP): Early attempt to provide security with the 8002.11 network protocol. 1999 -2004: Easy to break and hard to configure.
- Wi-Fi Protected Access (WPA, WPA2 and WPA3): Created to resolve issues with WEP.
- WPA was used as a temporary enhancement for WEP. Easy to break and moderate configuration difficulty.
- WPA2 (version 2): Provides good security and offers normal level of configuration. It was introduced in 2004. It used AES for encryption.
- WPA3: Next Generation Wireless Protocols: Offers excellent security and easy to configure.

SUMMARY

- Cryptography and encryption provide sophisticated approach to security.
- Many security-related tools use embedded encryption technologies.
- Encryption converts a message into a form that is unreadable by the unauthorized.
- Many tools are available and can be classified as symmetric or asymmetric, each having advantages and special capabilities.
- Strength of encryption tool is dependent on the key size but even more dependent on following good management practices.
- Cryptography is used to secure most aspects of Internet and Web today.