

Chapter 3

d42b4b5c2b78b389b1b8e
02fee0aba13d28d6389

By

TW9oZCBaYWtp==

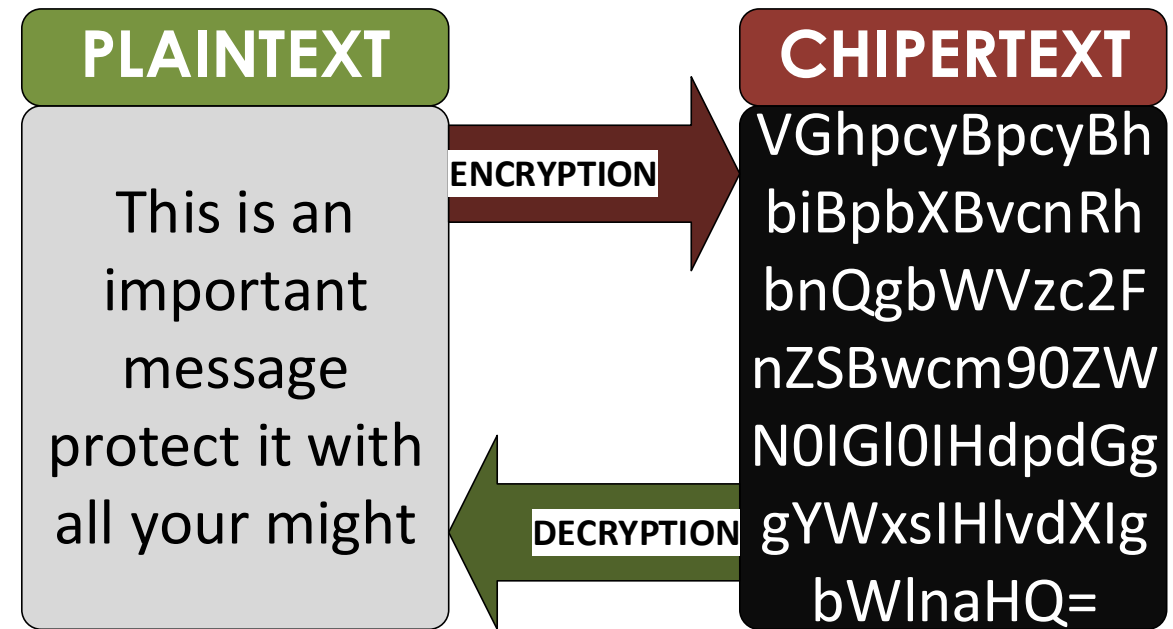
Content

- Concept Of Cryptography
- Cryptography Algorithm
- Cryptography Tool
- Cryptography Attacks

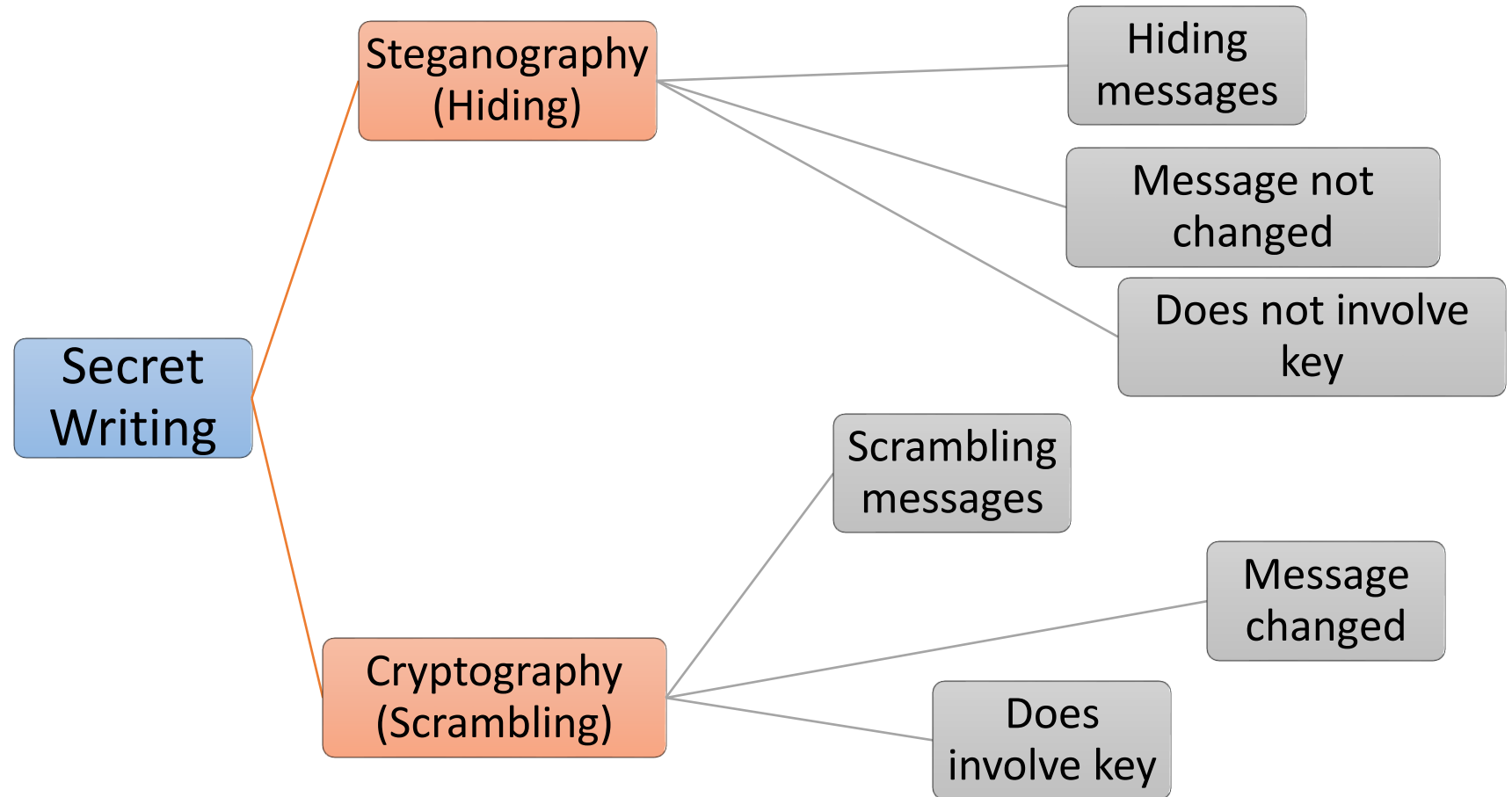
Concept of Cryptography

Concept Of Cryptography

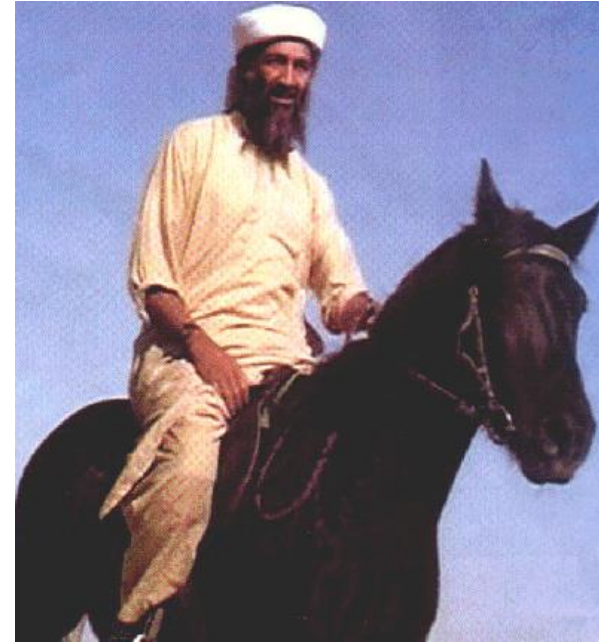
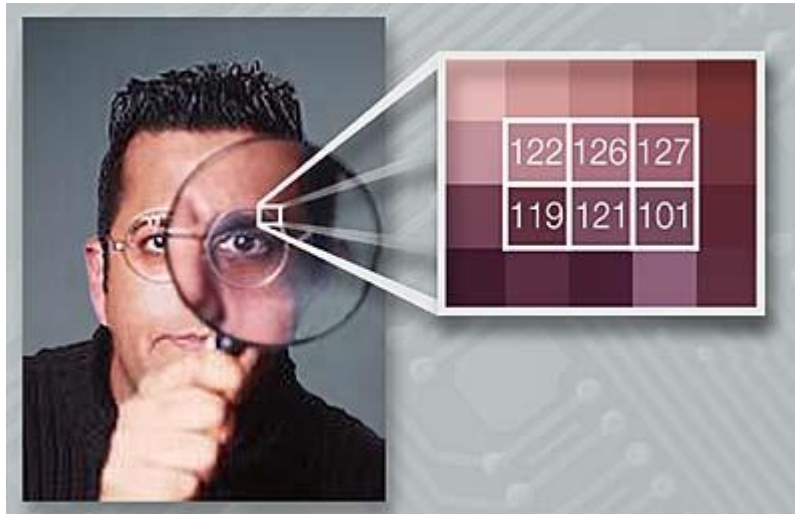
- The idea of a Cryptography is to disguise information in such a way that its meaning is unintelligible to an unauthorized person.
- The two most common uses are, probably, to store data securely in a computer file or to transmit it across an insecure channel such as the internet.
- Encrypted document does not prevent unauthorized people gaining access to it but, rather, ensures that they cannot understand what they see.



Secret writing



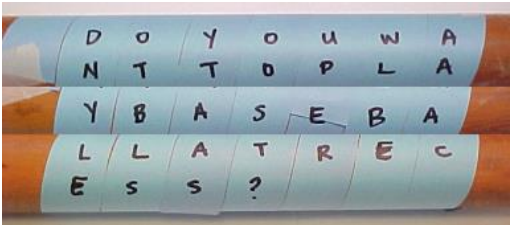
STEGANOGRAPHY -THE ART OF HIDING



Common methods include shaving you head bold, write something on it and wait for the hair to grow back.

Example of modern stegano methods is watermarking

THE EARLIEST INFORMATION SECURITY TOOL



THE SCYTALE

MECHANICAL CRYPTO MACHINE IN WORLD WAR II



- The Enigma machine.
- During its height, it was thought to be invincible.
- It was believed to be un-crackable.

PEOPLE BREAKING ENIGMA



In December 1932, a 27-year-old Polish mathematician, Marian Rejewski, who had joined the Polish Cipher Bureau in September that year, made one of the most important breakthroughs in cryptologic history by using algebraic mathematical techniques to solve the Enigma wiring.



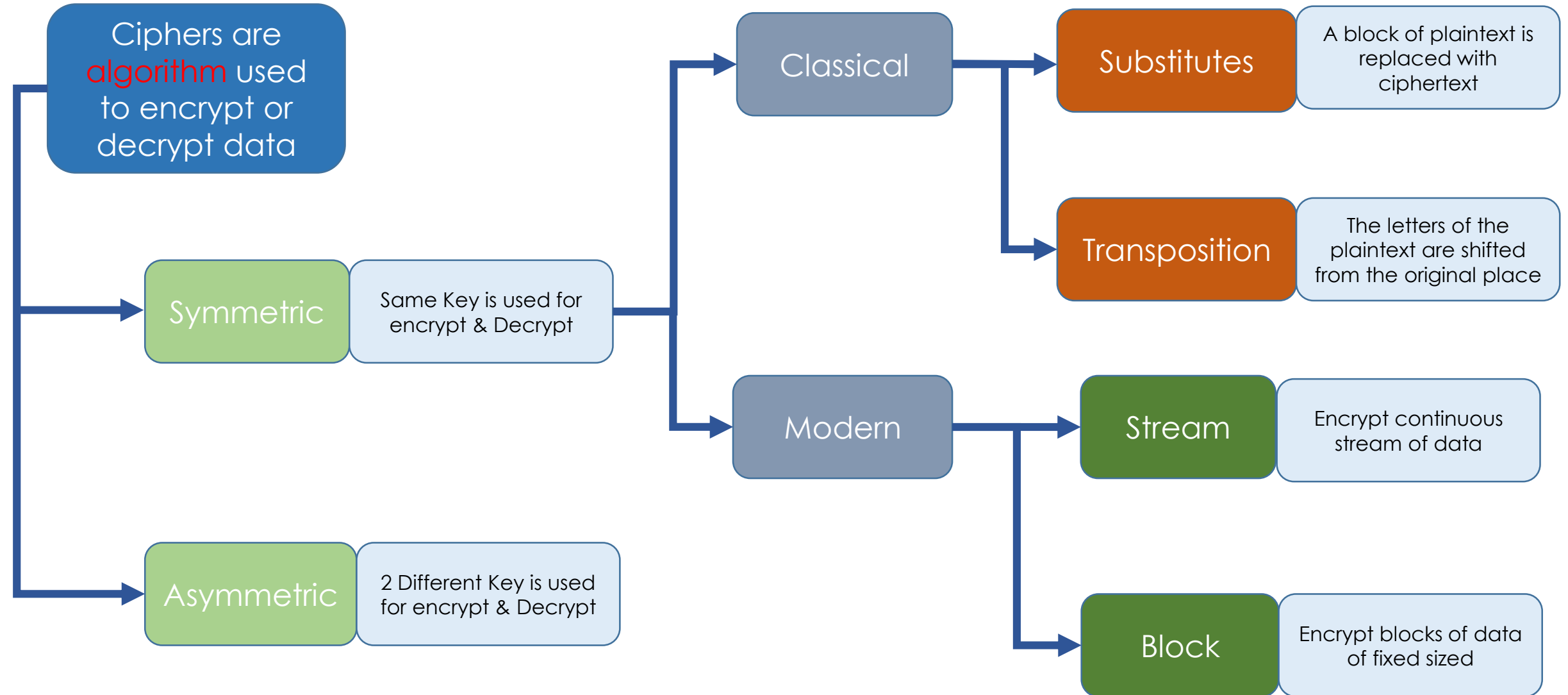
During the Second World War, Alan Turing was a main participant in the efforts at Bletchley Park to break German ciphers. Building on cryptanalysis work carried out in Poland by Marian Rejewski, Jerzy Różycki and Henryk Zygalski from Cipher Bureau before the war, he contributed several insights into breaking both the Enigma machine and the Lorenz SZ .

Cryptography Terminology

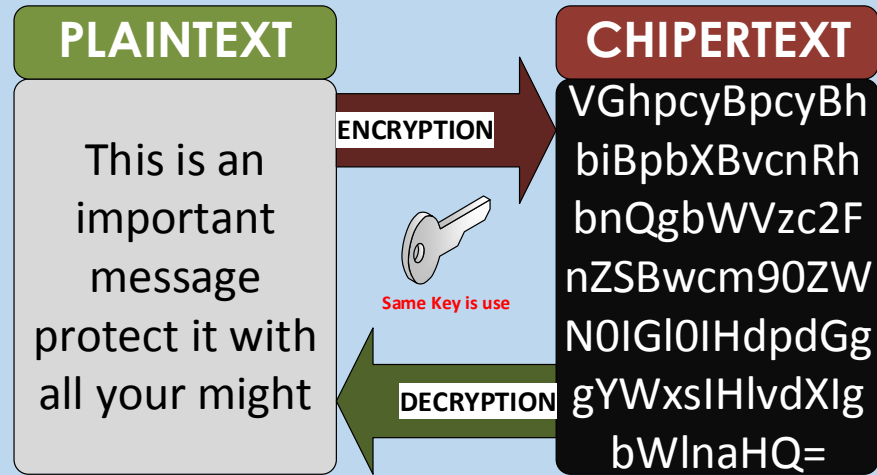
- **plaintext** - original message
- **ciphertext** - coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis

Cryptography Algorithm

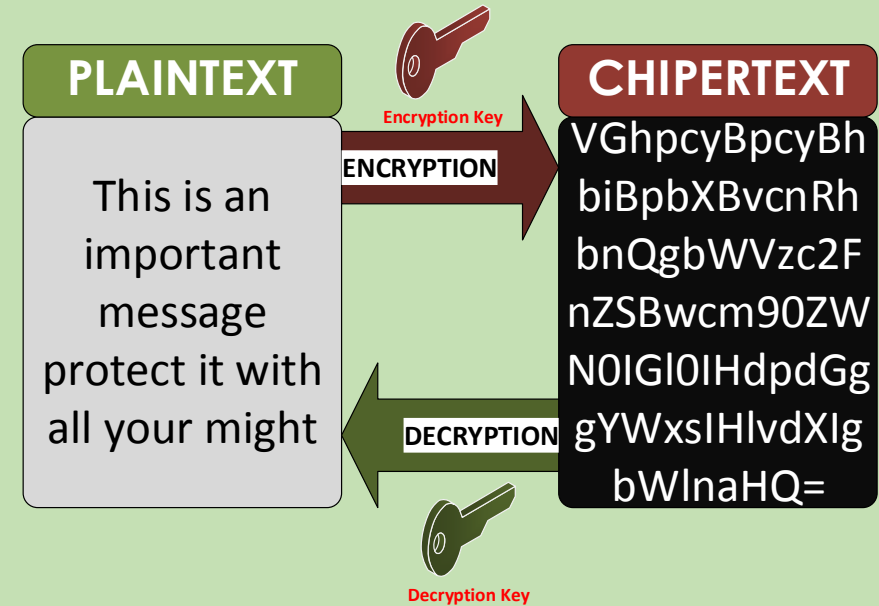
Cryptography Algorithms



Symmetric VS Asymmetric



- ❑ Symmetric algorithms $P=D(K,E(K,P))$
- ❑ If the system is **symmetric**, then there may be a need to distribute a secret key value before secret messages can be exchanged.
 - One of the most difficult aspects of obtaining a secure system.



- ❑ Asymmetric algorithms $P=D(K_d, E(K_e, P))$
- ❑ If the system is **asymmetric**, then it may be possible to avoid this particular problem by distributing only the encryption keys, which do not need to be secret.
 - However it is then replaced by the problem of guaranteeing the authenticity of each participant's encryption key.

Symmetric Cryptography Requirements

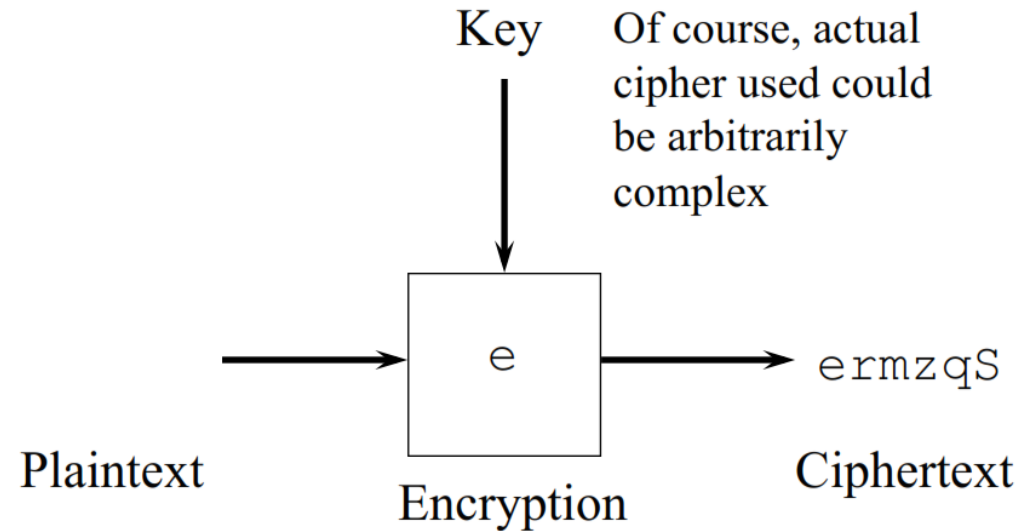
- two requirements for secure use of symmetric encryption:
 - a strong encryption algorithm
 - a secret key known only to sender / receiver
- mathematically have:
 - $C = E_K(P)$
 - $P = D_K(C)$
- assume encryption algorithm is known
- implies a secure channel to distribute key

Public-Key Cryptography (Asymmetric) Principles

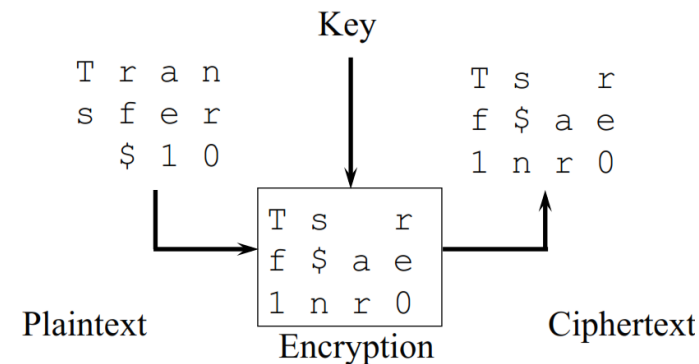
- The use of two keys has consequences in:
 - key distribution, confidentiality and authentication.
- The scheme has six ingredients
 - Plaintext
 - Encryption algorithm
 - Public key
 - Private key
 - Ciphertext
 - Decryption algorithm

Stream cipher

- Stream ciphers convert one symbol of plaintext immediately into one symbol of ciphertext
- Block ciphers work on a given sized chunk of data at a time



Block Ciphers



Methods use in Cryptography Algorithm

- Substitution
 - monoalphabetic substitution
 - Formed by shifting the letters of the original alphabet
 - polyalphabetic substitution
 - Extension of monoalphabetic substitution system
 - Using Vigenere Tableau
- Transposition
 - unkeyed transposition
 - Rearrange letters by using matrix
 - keyed transposition
 - Rearrange letters by using matrix where the size of matrix is determined by the length of the key used.

Well known Cipher

Caesar Cipher

- named after Julius Caesar, who used it to communicate with his generals.
- It is also known as the shift cipher, Caesar's code or Caesar shift.
- It is one of the simplest and most widely known encryption techniques.
- Letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.
- Example Key is 3

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
CipherText	D	E	F	G	H	I	J	K	L	M	N	O	P

Plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CipherText	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Plain text is =“WELCOME”

Cipher text is =“ZHOFRPH”

Caesar Cipher

Encryption

- Encryption of a letter x by a shift n can be described mathematically as,
 - $En(x) = (x+n) \bmod 26$
- Example:
 - Encryption of a letter A by a shift 3 can be described mathematically as,
 - $En(x) = (A+3) \bmod 26 = (0+3) \bmod 26 = 3 \bmod 26 = 3$
 - Encrypted letter for A is D

Decryption

- Decryption of a letter x by a shift n can be described mathematically as, Decryption is performed similarly,
 - $Dn(x) = (x-n) \bmod 26$
- Example:
 - Decryption of a letter D by a shift 3 can be described mathematically as,
 - $Dn(x) = (D-3) \bmod 26 = (3-3) \bmod 26 = 0 \bmod 26 = 0$
 - Decrypted letter for D is A

Caesar Cipher

- Caesar ciphers are vulnerable to exhaustive key search attack.
- To work through all the 26 keys.
- Furthermore the key can be determined from knowledge of a single pair of corresponding plaintext and ciphertext characters.

Find The message behind this cipher text

**YMJ KPJQ UWNHJ BNQQ
NSHWJFXJ YT WH KTZW
GD SJCY BJJP**

Caesar Cipher Exhaustive Key Search: cryptogram XMZVH

Enciphering key	Assumed message	Enciphering key	Assumed message	Enciphering key	Assumed message
0	XMZVH	17	GVIEQ	8	PERNZ
25	YNAWI	16	HWJFR	7	QFSOA
24	ZOBXJ	15	IXKGS	6	RGTPB
23	APCYK	14	JYLHT	5	SHUQC
22	BQDZL	13	KZMIU	4	TIVRD
21	CREAM	12	LANJV	3	UJWSE
20	DSFBN	11	MBOKW	2	VKXTF
19	ETGCO	10	NCPLX	1	WLYUG
18	FUHDP	9	ODQMY		

Mono-Alphabetic cipher

- Mono-Alphabetic cipher substitution technique
- It uses fixed substitution over the entire message
- Uses random substitution
- Requires permutation or combination of 26 alphabets.
- Hard to crack

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
CipherText	D	A	Q	S	H	P	J	R	L	X	N	Z	O

Plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CipherText	B	V	E	T	U	F	C	I	Y	M	K	W	G

Vigenere Cipher

- The Vigenère Cipher (the best known of the manual polyalphabetic cipher) uses a Vigenère Square to perform encryption.
- The left-hand (key) **column** of this square contains the English alphabet and for each letter, the **row** determined by that letter contains a rotation of the alphabet with that letter as the leading character.
 - So each letter in the left-hand column gives a Caesar Cipher whose shift is determined by that letter.
 - Example: the letter g gives the Caesar Cipher with shift 6.

Vigenere Table

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

Example: Polyalphabetic Substitution Cipher

Based on Vigenere, get the ciphertext for the plaintext “**A minutes success pays the failure of years**” in 4-letter words and “**failure**” as the repeating key. Use ‘x’ to pad out the blanks.

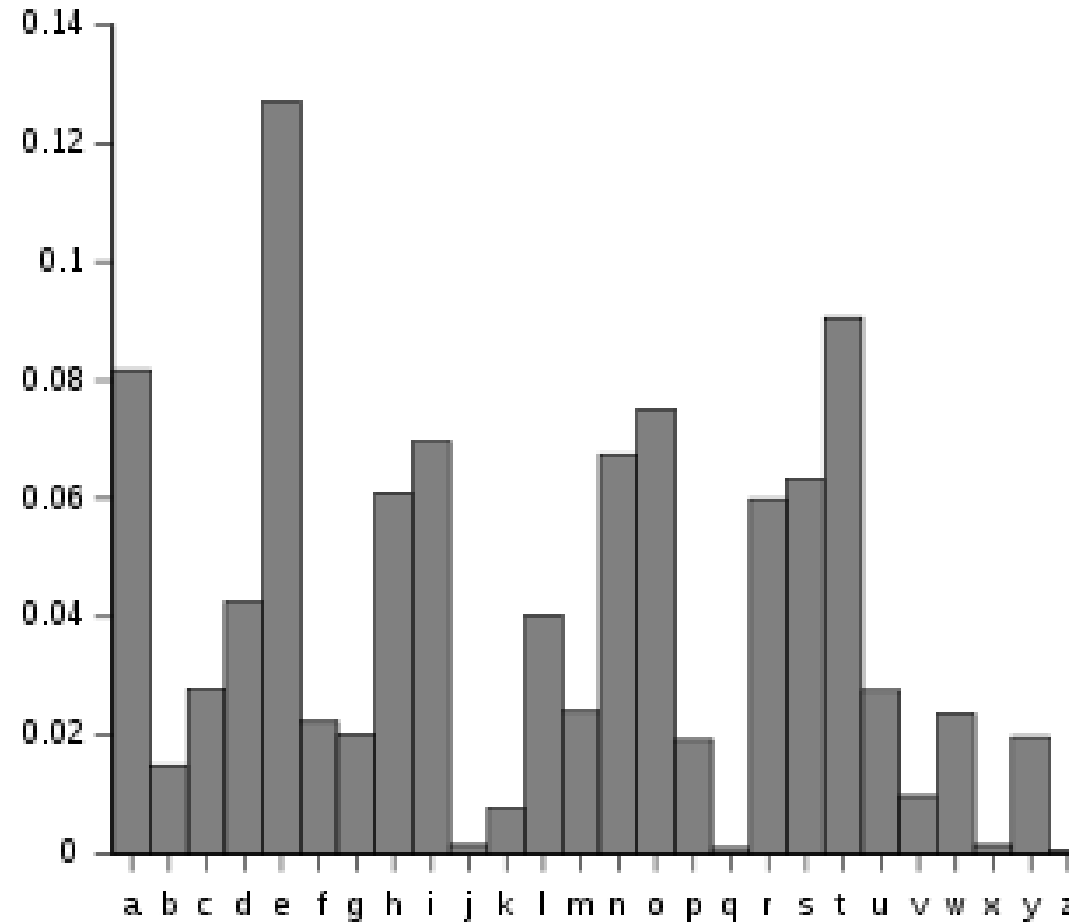
WHAT IS FREQUENCY ATTACK??

- First successful formal attack on ciphers was established by
- Al-Kindi (801-873).
- It was probably religiously motivated textual analysis of the Qur'an
- which led to the invention of the frequency analysis technique for
- breaking monoalphabetic substitution ciphers by al-Kindi sometime
- around AD 800.



The first page of al-Kindi's manuscript *On Deciphering Cryptographic Messages*, containing the oldest known description of cryptanalysis by frequency analysis.

LET US LOOK AT THE FREQUENCY OF THE ENGLISH ALPHABET



Breaking vigenere cipher

This cipher was secure from about 1553 till 1854 (301 years!!!)

- a. In 1854 Charles Babbage developed a test that succeeded to attack this cipher.
- b. In 1863 Friedrich Kasiski was the first to *publish* a successful attack on the Vigenère cipher.
- c. The primary weakness of the Vigenère cipher is the repeating nature of its key.

Transposition

- Letter is rearranged
- Letter are retain but moved from its position
- Two type
 - Unkeyed single transposition
 - Keyed single transposition

Modern Algorithms

- Most modern ciphers use a sequence of binary digits (bits), that is, zeros and ones such as ASCII.
- This bit sequence representing the plaintext is then encrypted to give the ciphertext as a bit sequence.
- The encryption algorithm may act on a bit-string in a number of ways.
 - *stream ciphers* where the sequence is encrypted bit-by-bit.
 - *block ciphers*, where the sequence is divided into blocks of a predetermined size.
 - ASCII requires 8 bits to represent one character, and so for a block cipher that has 64-bit blocks, the encryption algorithm acts on eight characters at once.

Data Encryption Standard (DES)

- The algorithm is designed to encipher and decipher block of data consisting 64 bits under control of a 56-bit key
- DES is the archetypal block cipher – an algorithm that takes a fixed length string of plaintext bits and transforms it into a ciphertext bitstring of the same length
- Due to inherent weaknesses of DES with today's technologies, some organizations repeat the process three times (3DES) for added strength, until they can afford to update their equipment to AES capabilities.

Advanced Encryption Standard (AES)

- AES is a symmetric-key algorithm for securing sensitive but unclassified material by U.S government agencies
- AES is an iterated block cipher, which works by repeating the same operation multiple times
- It has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively for AES 128, AES 192 and AES 256

AES Pseudocode

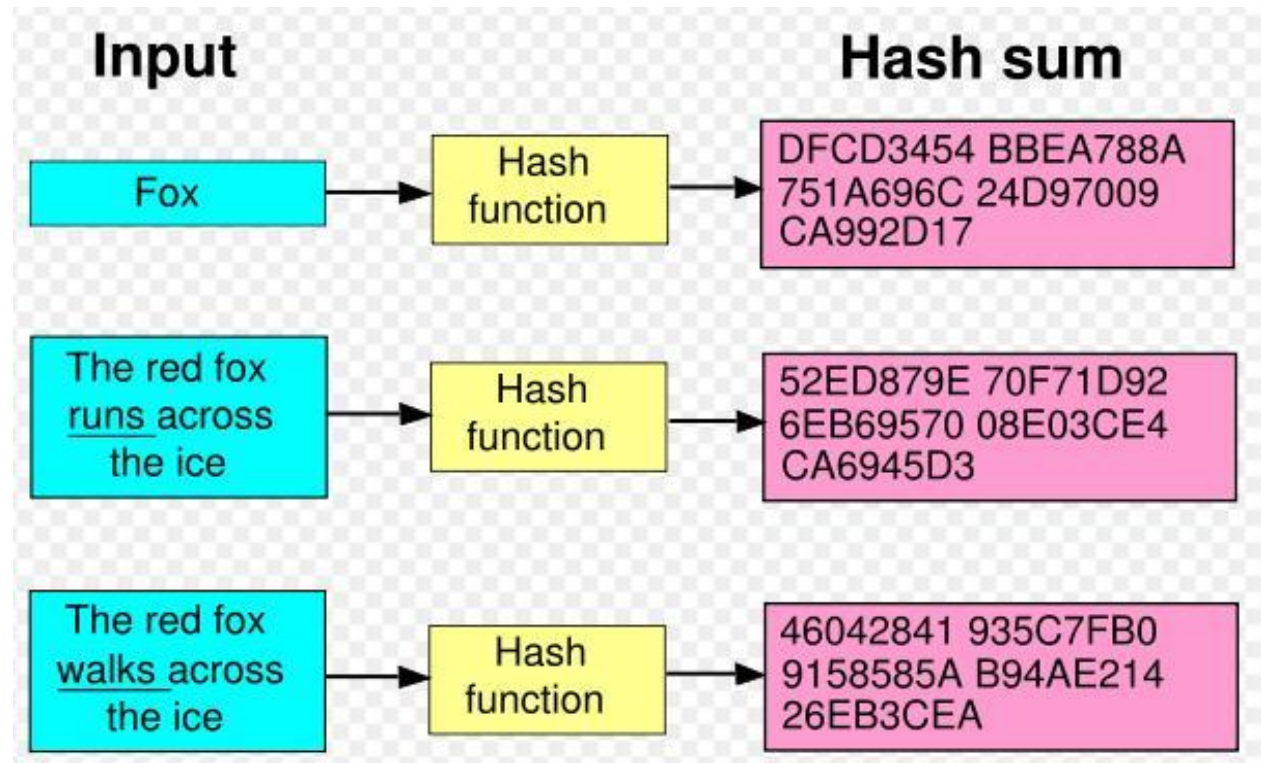
```
Cipher (byte in[4*Nb], byte out[4*Nb],  
word w[Nb*(Nr+1)])  
begin  
    byte state[4,Nb]  
    state = in  
    AddRoundKey(state, w)  
    for round = 1 step 1 to Nr-1  
        SubBytes(state)  
        ShiftRows(state)  
        MixColumns(state)  
        AddRoundKey(state, w+round*Nb)  
    end for  
    SubBytes(state)  
    ShiftRows(state)  
    AddRoundKey(state, w+Nr*Nb)  
    out = state  
end
```

RC4, RC5, RC6 Algorithm

- RC4 A variable key size stream cipher with byte oriented operations, and is based on the use of a random permutation
- RC5 It is a parameterized algorithm with a variable key size, and a variable number of rounds. The key size is 128-bits
- RC6 is a symmetric key block cipher derived from RC5 with two additional features:
 - Uses Integer multiplication
 - Uses 4-bit working registers (RC5 uses two 2-bit registers)

Message Digest (One Way Hash)

- Hash Function calculate a unique fixed-size bit string representation called a message digest of any arbitrary block of information
- If any given bit of function's input is changed. Every output bit has a 50% chance of changing
- It is computationally infeasible to have two files with the same message digest value



Base64 encoding and decoding

Digital Signature

- DS is computed a set of rules and a set of parameters such that the identity of the signatory and integrity of the data can be verified
- FIPS 186-2 specifies DS Algorithm that may be used in the generation and verification of digital signatures for sensitive, unclassified application

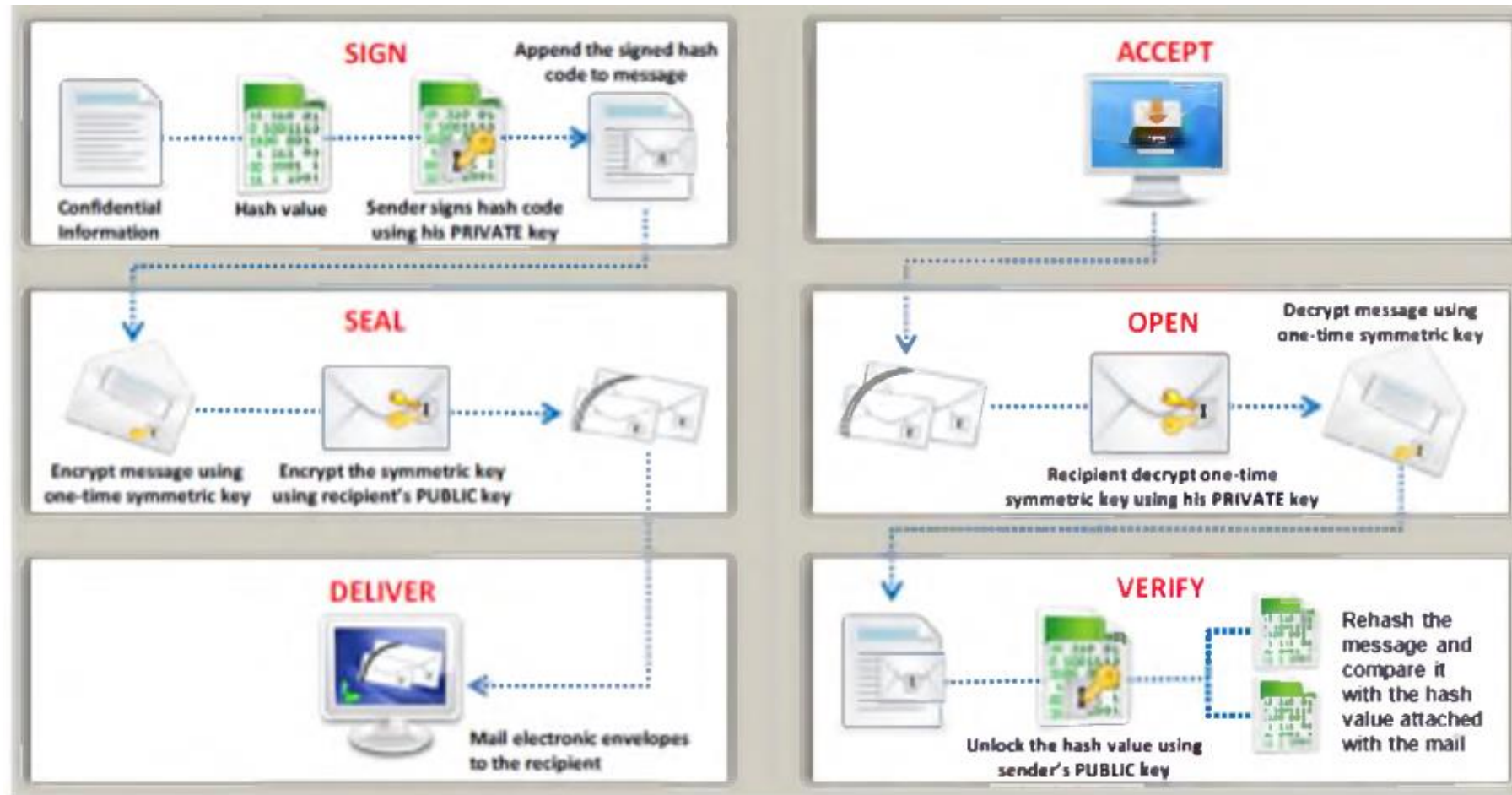
Each entity creates a public key and corresponding private key

1. Select a prime number q such that $2^{159} < q < 2^{160}$
2. Choose t so that $0 \leq t \leq 8$
3. Select a prime number p such that $2^{511+64t} < p < 2^{512+64t}$ with the additional property that q divides $(p-1)$
4. Select a generator α of the unique cyclic group of order q in Z_p^*
5. To compute α , select an element g in Z_p^* and compute $g^{(p-1)/q} \bmod p$
6. If $\alpha = 1$, perform step five again with a different g
7. Select a random a such that $1 \leq a \leq q-1$
8. Compute $y = \alpha^a \bmod p$



The public key is (p, q, α, y) . The private key is a .

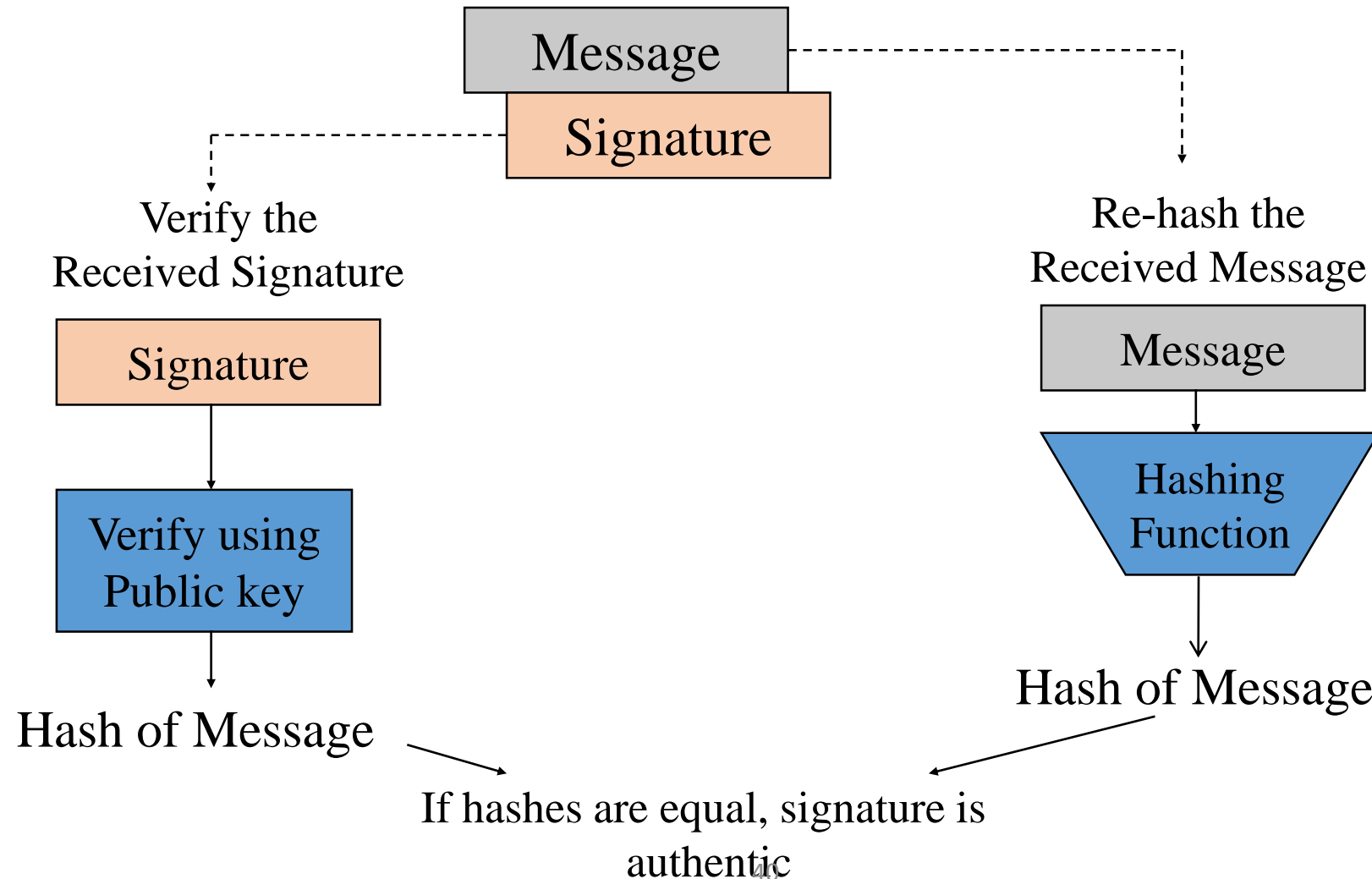
HOW DS works



Verifying a Digital Signature

- The signature can be verified by anyone who knows the corresponding public key.
- To do this a value is produced from the signature using the asymmetric algorithm with the public key.
- This value should be the hash of the message, which anyone can calculate.
- If this value and the hash agree, the signature is accepted as genuine.

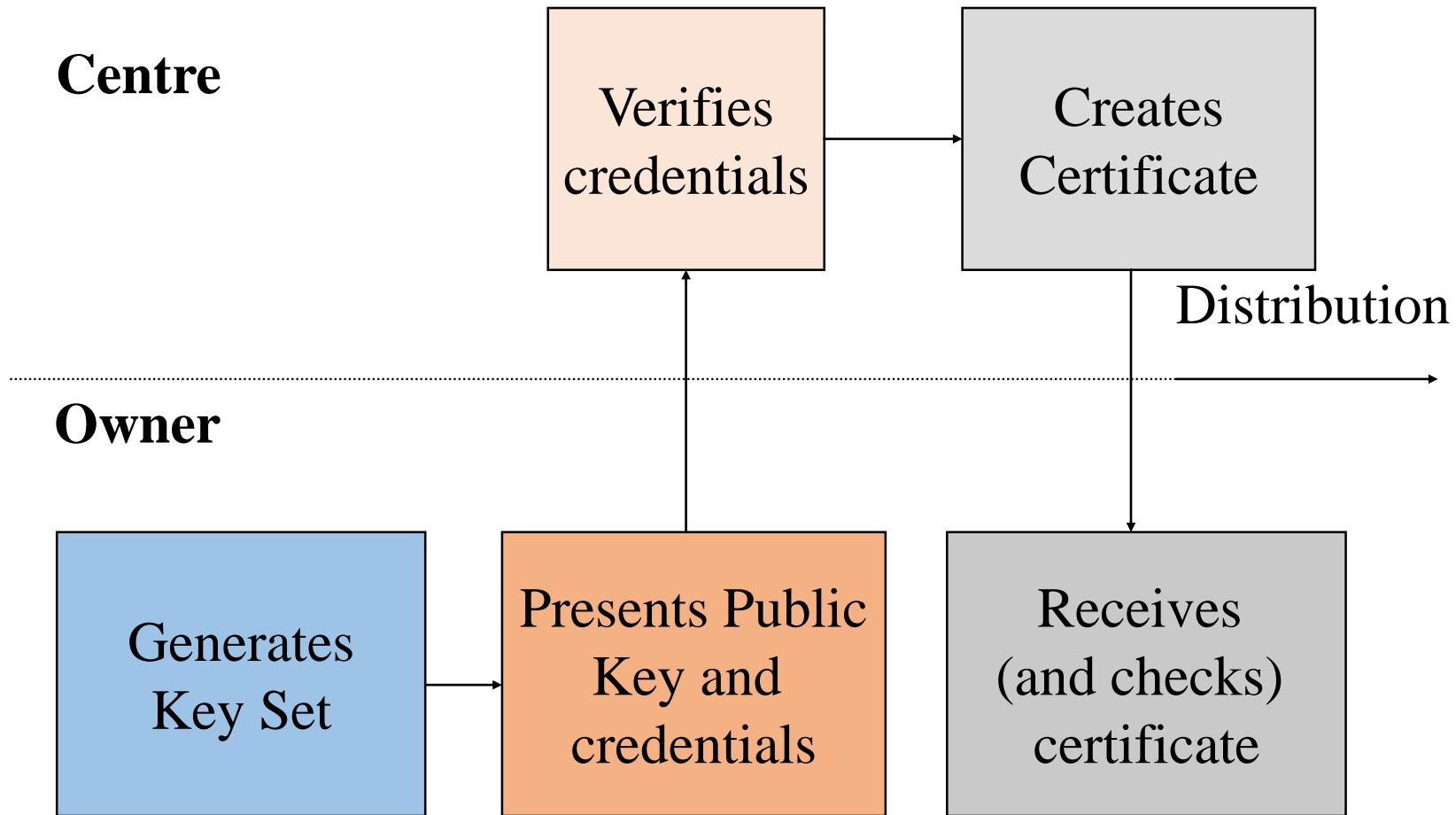
How to Verify a Digital Signature Using RSA



Certification Authority (CA)

- AIM:
 - To guarantee the authenticity of public keys.
- METHOD:
 - The CA guarantees the authenticity by signing a certificate containing user's identity and public key with its secret key.
- REQUIREMENT:
 - All users must have an authentic copy of the Certification Authority's public key.

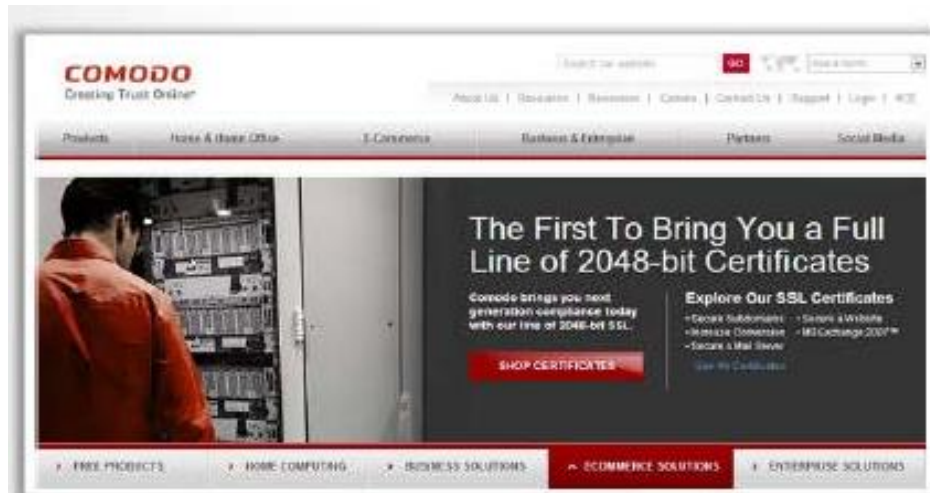
Certification Process



How Does it Work?

- The certificate can accompany all sender's messages.
- The recipient must directly or indirectly:
 - Trust the CA
 - Validate the certificate

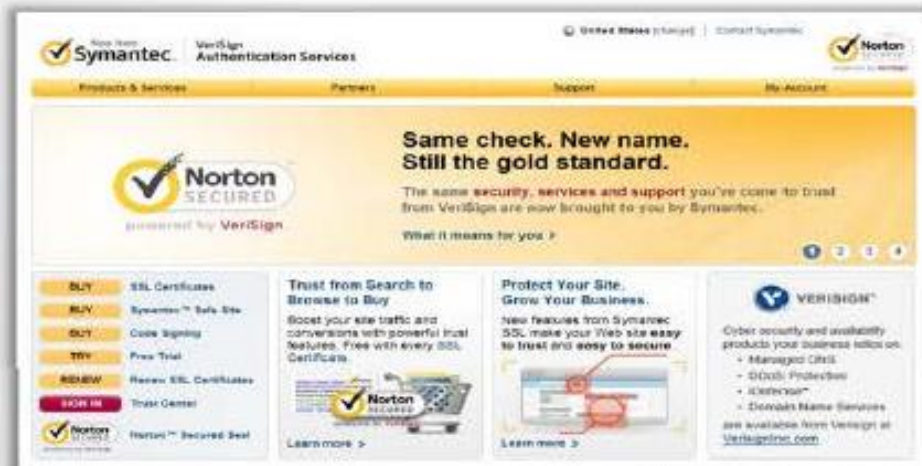
Certification Authorities



<http://www.comodo.com>



<http://www.thawte.com>



<http://www.symantec.com>



<http://www.entrust.net>

Certification Authorities

- Problems / Questions
 - Who generates users' key?
 - How is identity established?
 - How can certificates be cancelled?
 - Any others?

Attacks on Digital Signature

- Suppose digital signatures are being used as a means of identification.
- If user A wishes to impersonate user B, then there are two different forms of attack:
 - A attempts to obtain the use of B's private key
 - A tries to substitute their public key for B's public key.

Public Key Infrastructure (PKI)

- The motivation of using PKI is to facilitate the use of public key cryptography.
- Three key players in PKI system:
 - The certificate owner - who applies for the certificate.
 - CA - which issues the certificate that binds the owner's identity to the owner's public key value.
 - The relying party - who uses on the certificate.
- Other players:
 - *Registration Authority (RA)* - in some systems the identification verification is performed by a separate authority.
 - *Validation Authority (VA)* - end users ask the VA if a given certificate is still valid and receive a yes or no answer.

Establishing a PKI

- When a PKI is established, the following processes need to take place:
 - The key pairs for CAs must be generated.
 - The key pairs for users must be generated.
 - Users must request certificates
 - Users' identities must be verified.
 - Users' key pairs must be verified.
 - Certificates must be produced.
 - Certificates must be checked.
 - Certificates must be removed/updated (when necessary).
 - Certificates must be revoked (when necessary).

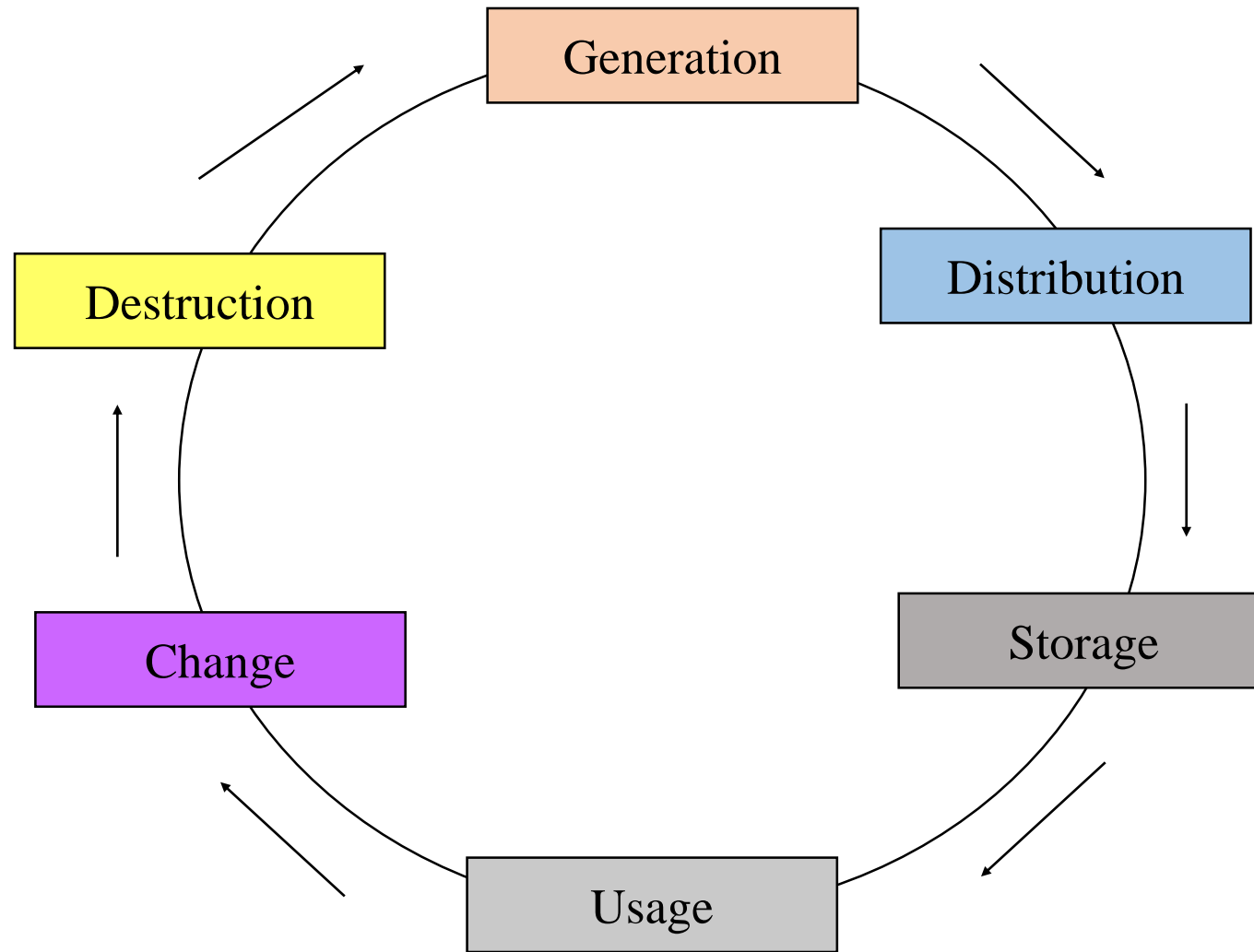
Key Management

- A typical requirement specification for a symmetric key system might include each of the following:
 - Keys must be generated using a random or pseudorandom process.
 - Any key used by a communicating pair must be unique to them.
 - A key must be used for only for a purpose, e.g. the same key should not be used for both encryption and authentication.
 - Each key must be replaced within the time deemed necessary to determine it by an exhaustive search.

Key Management (Cont.)

- A key must not be used if its compromise is either known or suspected.
- Compromise of a key which is shared between two parties must not compromise any key used by a third party.
- Keys should only appear in clear form within a highly tamper resistant device. Elsewhere all keys must be encrypted or in component form.
- Keys must be protected against misuse.
- Unauthorized modification, substitution or replay of any key must be prevented or detected.

The Key Life Cycle



RSA Algorithm

- RSA (Rivest Shamir Adleman)
- An Internet encryption and authentication system that uses an algorithm developed by Rivest, Adi Shamir and Leonard Adleman
- Widely used and is one of the de facto standards
- Uses modular arithmetic and elementary number theories to perform computations using two large prime numbers

p, q , two prime numbers

(private, chosen)

$$n = p * q$$

(public, calculated)

e , with $\gcd(\phi(n), e) = 1$;
 $1 < e < \phi(n)$

(public, chosen)

$$d = e^{-1} \pmod{\phi(n)}$$

(private, calculated)

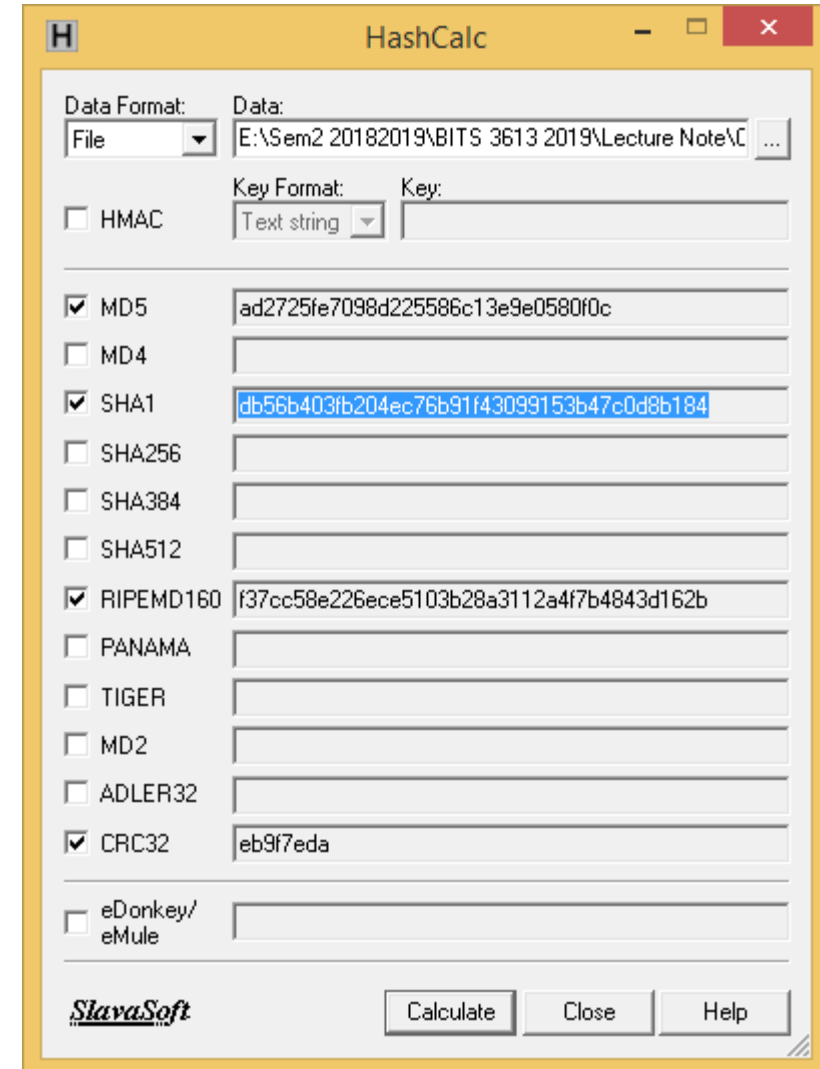
RSA

- each user generates a public/private key pair by:
- selecting two large primes at random - p, q
- computing their system modulus $n=p*q$
 - note $\phi(n) = (p-1)(q-1)$
- selecting at random the encryption key e
 - where $1 < e < \phi(n)$,
 $\gcd(e, \phi(n)) = 1$
- solve following equation to find decryption key d
 - $e*d = 1 \bmod \phi(n)$ and $0 \leq d \leq n$
- publish their public encryption key: $PU = \{e, n\}$
- keep secret private decryption key: $PR = \{d, n\}$
- to encrypt a message M the sender:
 - obtains public key of recipient $PU = \{e, n\}$
 - computes: $C = M^e \bmod n$, where $0 \leq M < n$
- to decrypt the ciphertext C the owner:
 - uses their private key $PR = \{d, n\}$
 - computes: $M = C^d \bmod n$
- note that the message M must be smaller than the modulus n (block if needed)

Crypto Tool

Hash Calculator

- MD5 calculator
- Hash Calculator
- Advanced Encryption Package
- BCTextEncoder



Cryptography Tool



AutoKrypt

<http://www.hiteksoftware.com>



NCrypt XL

<http://www.littlelite.net>



**Cryptainer LE Free
Encryption Software**

<http://www.cypherix.com>



ccrypt

<http://ccrypt.sourceforge.net>



Steganos LockNote

<https://www.steganos.com>



WinAES

<http://fatlyz.com>



AxCrypt

<http://www.axantum.com>



EncryptOnClick

<http://www.2brightsparks.com>



CryptoForge

<http://www.cryptoforge.com>



GNU Privacy Guard

<http://www.gnupg.org>

Disk Encryption Tool

- Protects confidentiality of the data stored on disk by converting data into unreadable code using disk encryption software or hardware
- Work similar way as text message encryption and protect data even when OS not active.
- Can safeguard any information to be burn onto the disk and keep it from falling into the wrong hands.



Cryptography attacks

Cryptography Attacks

- Based on the assumption that the cryptanalyst has access to the encrypted information.
 - Ciphertext only
 - Known plaintext attack
 - Chosen plaintext
 - Chosen ciphertext attack
 - Chosen key attack
 - Adaptive chosen plaintext attack
 - Timing attack
 - Rubber hose attack

Ciphertext only attack

- Attacker has access to the cipher text
- Goal of this attack is to recover encryption key from the ciphertext

Adaptive Chosen plaintext attack

- Attacker make a series of interactive queries
- Choosing subsequent plaintexts based on the information from the previous encryptions

Chosen Plaintext Attack

- Attacker defines his own plaintext, feeds it into the cipher and analyzes the result ciphertext

Known plaintext Attack

- Attacker has knowledge of some part of the plain text
- Using this information the key used to generate ciphertext is deduced so as to decipher other messages

Chosen ciphertext Attack

- Attacker obtains the plaintexts corresponding to an arbitrary set of ciphertexts of his own choosing

Rubber Hose Attack

- Extraction of cryptographic secrets from a person by coercion or torture

Chosen key attack

- A generalization of the chosen text attack

Timing attack

- It is based on repeatedly measuring the exact execution times of modular exponentiation operations

Code Breaking Methodology

Trickery and Deceit

- Use of social engineering techniques to extract cryptography keys

Brute Force

- Cryptography keys are discovered by trying every possible combination

One-Time Pad

- Contains many non-repeating groups of letters or number keys which are chosen randomly

Frequency Analysis

- It is the study of the frequency of letters or groups of letters in a ciphertext
- It works on the fact that, in any given stretch of written language , certain letters and combination of letters occur with varying frequencies

Brute Force Attacks

Attack Scheme

- Defeating a cryptographic scheme by trying a large number of possible keys until the correct encryption key is discovered

Brute Force Attack











- Brute-force attack is a high resource and time intensive process, however, more certain to achieve results

Success Factors

- Success of brute force attack depends on length of the key, time constraint, and system security mechanisms

Power/Cost	40 bits (5 char)	56 bit (7 char)	64 bit (8 char)	128 bit (16 char)
\$ 2K (1 PC. Can be achieved by an individual)	1.4 min	73 days	50 years	10^{20} years
\$ 100K (this can be achieved by a company)	2 sec	35 hours	1 year	10^{19} years
\$ 1M (Achieved by a huge organization or a state)	0.2 sec	3.5 hours	37 days	10^{18} years

Cryptanalyst Tool

 CryptoBench http://www.addario.org	 AlphaPeeler http://alphapeeler.sourceforge.net
 JCrypTool http://www.cryptool.org	 Draft Crypto Analyzer http://www.literatecode.com
 Ganzúa http://ganzua.sourceforge.net	 Linear Hull Cryptanalysis of PRESENT http://www.ecrypt.eu.org
 Crank http://crank.sourceforge.net	 mediggo http://code.google.com
 EverCrack http://evercrack.sourceforge.net	 SubCypher http://www.esclepiusllc.com

Summary

Summary

- Cryptography is the conversion of data into a scrambled code that is sent across a private or public network and decrypted by its recipients
- Using Public Key Infrastructure (PKI), anyone can send a confidential message using public information, which can only be decrypted with a private-key in the sole possession of the intended recipient
- AES is a symmetric-key algorithm for securing sensitive but unclassified material by U.S. government agencies
- Cryptography attacks are based on the assumption that the cryptanalyst has access to the encrypted information
- Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates

