CSF3404 Cyber Security

Chapter 3
Cryptography

Lecturer:
Waheed Ghanem
Fakhrul Adli bin Mohd Zaki
Aalim Rozli

Faculty of Ocean Engineering Technology and Informatics,
Universiti Malaysia Terengganu

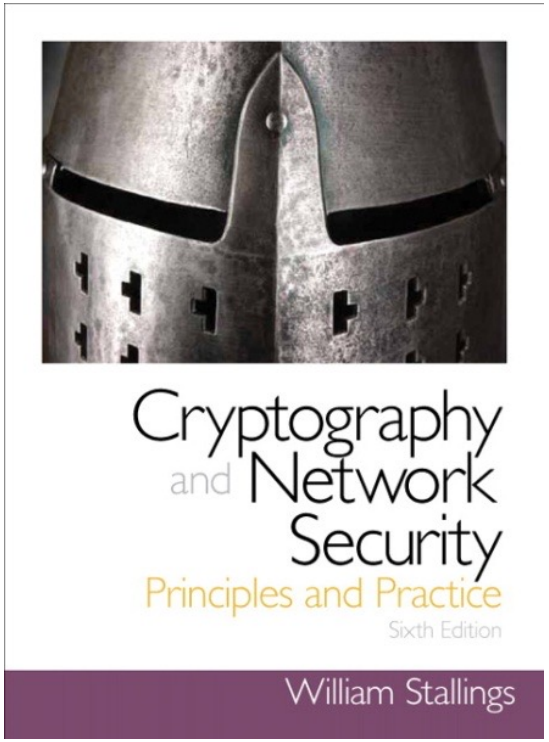
Cryptography and Network Security

We lead

Cryptography and Network Security

Sixth Edition

William Stallings

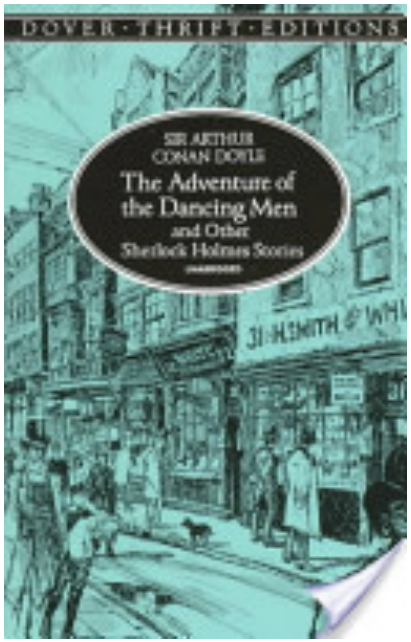


The Art of War

UMT
We lead

This quote is from The Art of War.

"I am fairly familiar with all the forms of secret writings and am myself the author of a trifling monograph upon the subject, in which I analyze one hundred and sixty separate ciphers," said Holmes.



—The Adventure of the Dancing Men,
Sir Arthur Conan Doyle

Cryptography

Cryptography is the science of hiding information. The practice of cryptography is thought to be nearly as old as the written word. Current cryptographic science has its roots in mathematics and computer science, and relies heavily upon technology. Modern communications and computing use cryptography extensively to protect sensitive information and communications from unauthorized access or accidental disclosure while the information is in transit and while the information is being stored.

G7JDZL	L539CZ	AA9CZ1
ZPQ12G	93L12B	LP7FFH
18ABHU	UJ[illegible]	334FYO
K71TYP	CS3[illegible]4	566HHX
SAPRW1	SP5[illegible]3S	3F8Y0K
PVF129	A7V[illegible]TT	ADL10M
N031M1	LAE3FB	1L598X
RX0FYT	LM2HU5	GT610A
I5581Z	QH1UNB	9JB70W

Note: The word cryptography has roots in the Greek words kryptós, meaning "hidden," and "gráphein," meaning "to write," translating to "hidden writing."

Cryptography

Cryptography

Cryptography is the **conversion of data** into a scrambled code that is decrypted and sent across a private or public network

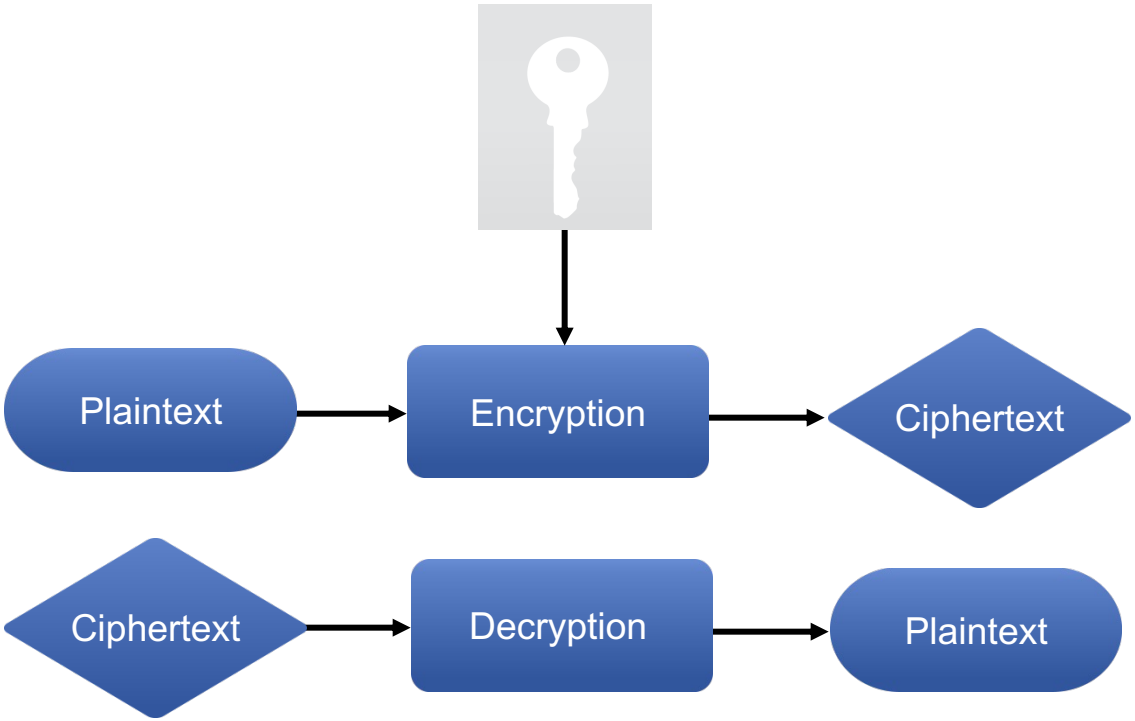
Cryptography is used to **protect** e-mail messages, credit card information, and corporate data

Objectives of Cryptography

1. Confidentiality
2. Integrity
3. Authentication
4. Non–Repudiation

Encryption and Decryption

Encryption is a cryptographic technique that converts data from *plaintext*, or *cleartext* form, into coded, or *ciphertext* form. *Decryption* is the companion technique that converts ciphertext back to cleartext.



Ciphers

Ciphers

Ciphers are algorithms used to encrypt or decrypt the data

Classical Ciphers

- **Substitution cipher** — It replaces bits, characters, or blocks of characters with different bits, characters or blocks
- **Transposition cipher** — The letters of the plaintext are shifted about to form the cryptogram

Modern Ciphers

Based on the type of key used

- **Private Key** — Same key is used for encryption and decryption
- **Public Key** — Two different keys are used for encryption and decryption

Based on the type of input data

- **Block Cipher** — Encrypts block of data of fixed size
- **Stream Cipher** — Encrypts continuous streams of data

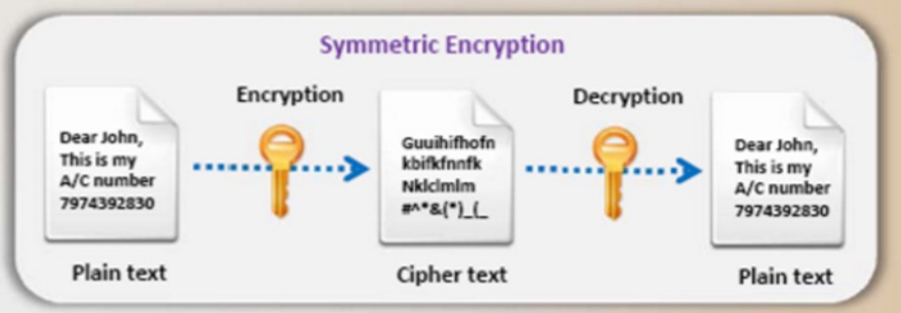
Types of Cryptography

UMT
We lead

Types of Cryptography

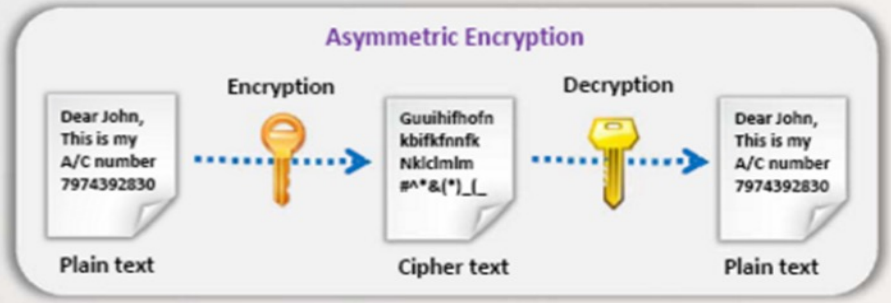
Symmetric Encryption

Symmetric encryption (secret-key, shared-key, and private-key) uses the same key for encryption as they do for decryption



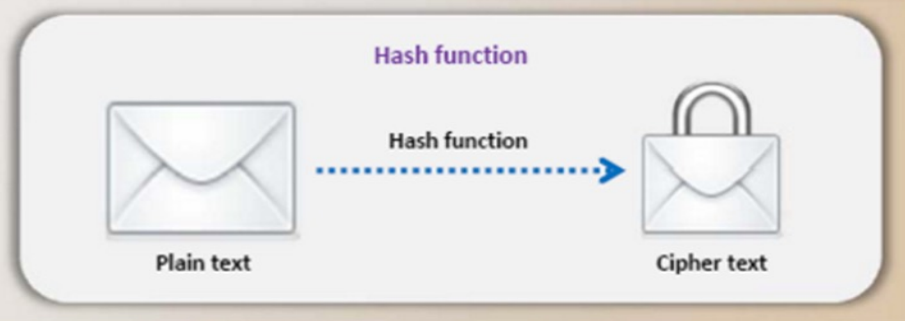
Asymmetric Encryption

Asymmetric encryption (public-key) uses different encryption keys for encryption and decryption. These keys are known as public and private keys



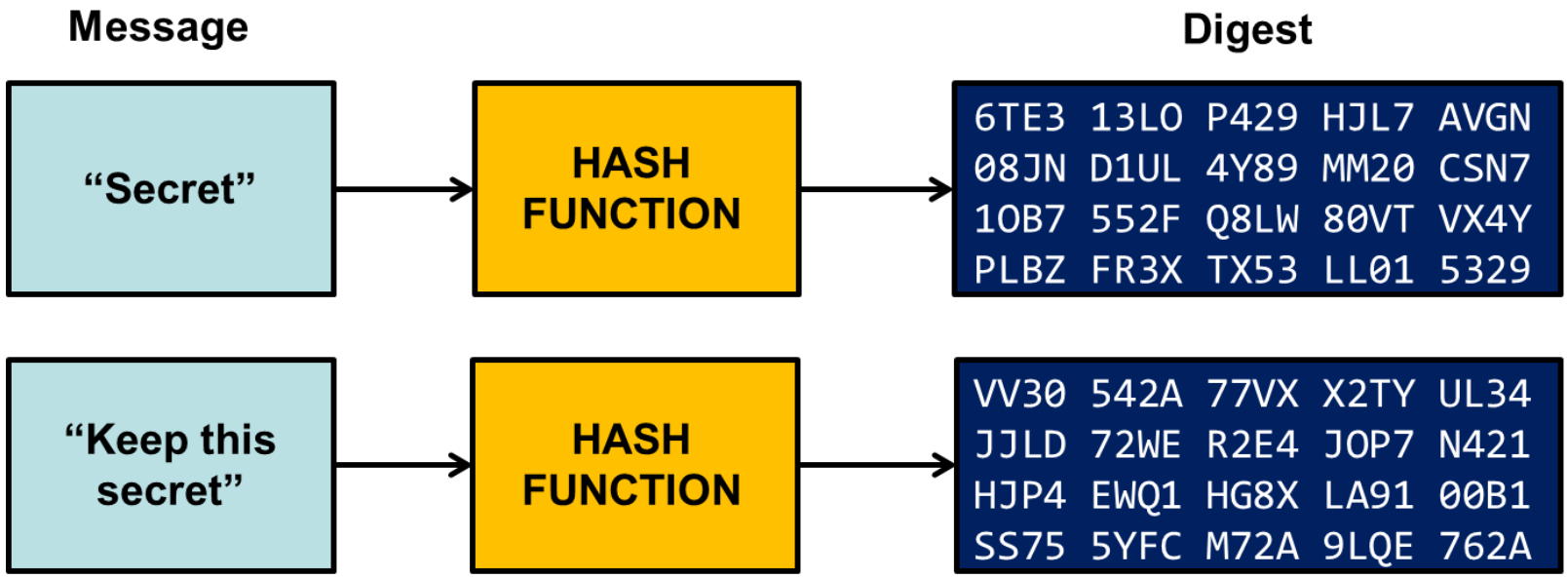
Hash Function

Hash function (message digests or one - way encryption) uses no key for encryption and decryption



Hashing Encryption

Hashing encryption is one-way encryption that transforms cleartext into ciphertext that is not intended to be decrypted. The result of the hashing process is called a *hash*, *hash value*, or *message digest*. The input data can vary in length, whereas the hash length is fixed.



Hashing Encryption Algorithms

UMT
We lead

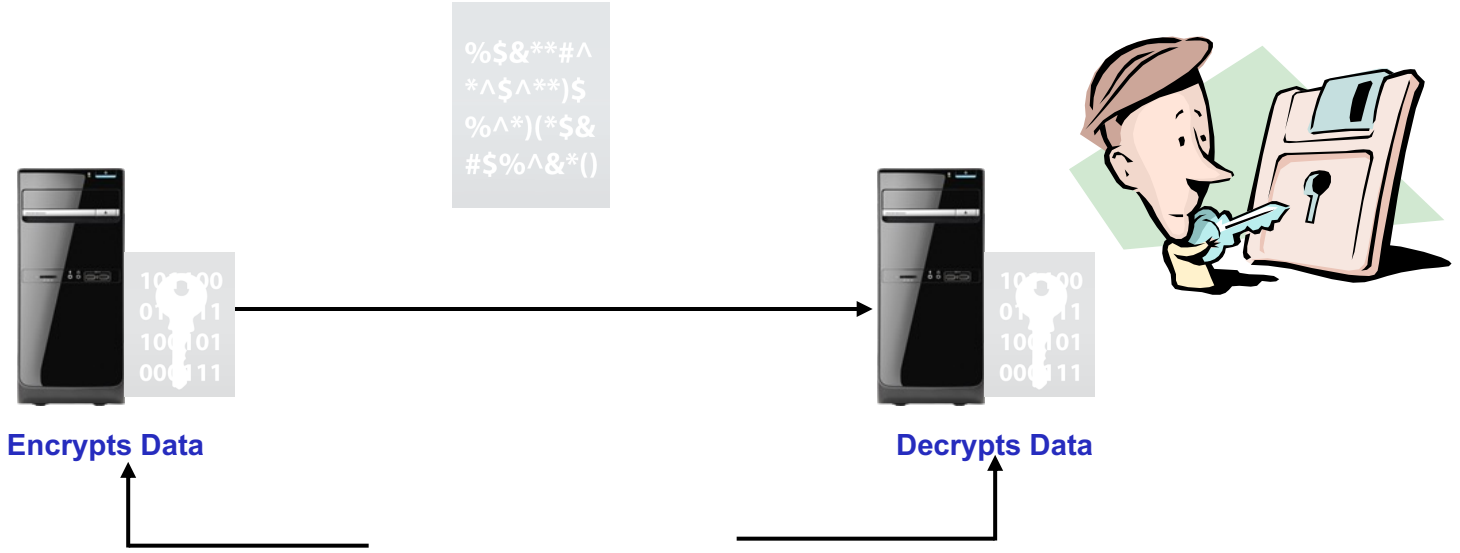
- MD5
- SHA
- NTLM versions 1 and 2
- RIPEMD
- HMAC

Hashing Encryption Algorithms

Hashing Algorithm	Description
Message Digest 5 (MD5)	This algorithm produces a 128-bit message digest. It was created by Ronald Rivest and is now in the public domain. MD5 is no longer considered a strong hash function.
Secure Hash Algorithm (SHA)	This algorithm is modeled after MD5 and is considered the stronger of the two. Common versions of SHA include SHA-160, which produces a 160-bit hash value, while SHA-256, SHA-384, and SHA-512 produce 256-bit, 384-bit, and 512-bit digests, respectively. Performance-wise, SHA is at a disadvantage to MD5.
NT LAN Manager (NTLM#)	NTLMv1 is an authentication protocol created by Microsoft® for use in its products and released in early versions of Windows® NT. NTLMv2 was introduced in the later versions of Windows NT.
RACE Integrity Primitives Evaluation Message Digest (RIPEMD)	This is a message digest algorithm (cryptographic hash function) that is based along the lines of the design principles used in *MD4*. There are 128, 160, 256, and 320-bit versions called RIPEMD-128, RIPEMD-160, RIPEMD-256, and RIPEMD-320, respectively. The 256- and 320-bit versions reduce the chances of generating duplicate output hashes but do little in terms of higher levels of security. RIPEMD-160 was designed by the open academic community and is used less frequently than SHA-1, which may explain why it is less scrutinized than SHA.
Hash-based Message Authentication Code (HMAC)	This is a method used to verify both the integrity and authenticity of a message by combining cryptographic hash functions, such as MD5 or SHA-1, with a secret key. The resulting calculation is named based on what underlying hash function was used. For example, if SHA-1 is the hash function, then the HMAC algorithm is named HMAC-SHA1.

Symmetric Encryption

- Also referred to as conventional encryption or single-key encryption
- all classical encryption algorithms are private-key
- Was the only type of encryption in use prior to the development of public-key encryption in the 1970s



Symmetric encryption is a two-way encryption scheme in which encryption and decryption are both performed by the same key. The key can be configured in software or coded in hardware. The key must be securely transmitted between the two parties prior to encrypted communications, which can prove difficult. Symmetric encryption is relatively fast, but is vulnerable if the key is lost or compromised. Some of the common names for symmetric encryption are secret-key, shared-key, and private-key encryption.

Symmetric Encryption Algorithms

We lead

- DES
- 3DES
- AES
- Blowfish
- Twofish
- RC 4, 5, 6

Symmetric Encryption Algorithms

UMT
We lead

Symmetric Algorithm	Description
Data Encryption Standard (DES)	A block-cipher symmetric encryption algorithm that encrypts data in 64-bit blocks using a 56-bit key with 8 bits used for parity. The short key length makes DES a relatively weak algorithm, though it requires less performance overhead.
Triple DES (3DES)	A symmetric encryption algorithm that encrypts data by processing each block of data three times using a different key each time. It first encrypts plaintext into ciphertext using one key, then encrypts that ciphertext with another key, and lastly encrypts the second ciphertext with yet another key. 3DES is stronger than DES, but also triples the performance impact.

Symmetric Encryption Algorithms

We lead

Advanced Encryption Standard (AES) algorithm	A symmetric 128-, 192-, or 256-bit block cipher developed by Belgian cryptographers Joan Daemen and Vincent Rijmen and adopted by the U.S. government as its encryption standard to replace DES. The AES algorithm is called Rijndael (pronounced "Rhine-dale") after its creators. Rijndael was one of five algorithms considered for adoption in the AES contest conducted by the National Institute of Standards and Technology (NIST) of the United States. AES is considered one of the strongest encryption algorithms available, and offers better performance than 3DES.
Blowfish	A freely available 64-bit block cipher algorithm that uses a variable key length. It was developed by Bruce Schneier. Blowfish is no longer considered strong, though it does offer greater performance than DES.
Twofish	A symmetric key block cipher, similar to Blowfish, consisting of a block size of 128 bits and key sizes up to 256 bits. Although not selected for standardization, it appeared as one of the five finalists in the AES contest. Twofish encryption uses a pre-computed encrypted algorithm. The encrypted algorithm is a key-dependent *S-box,* which is a relatively complex key algorithm that when given the key, provides a substitution key in its place. This is referred to as "n" and has the sizes of 128, 192, and 256 bits. One half of "n" is made up of the encryption key, and the other half contains a modifier used in the encryption algorithm. Twofish is stronger than Blowfish and offers comparative levels of performance.
Rivest Cipher (RC) 4, 5, and 6	A series of algorithms developed by Ronald Rivest. All have variable key lengths. RC4 is a stream cipher. RC5 and RC6 are variable-size block ciphers. RC6 is considered a strong cipher and offers good performance.

Asymmetric Encryption

UMT
We lead

Unlike symmetric encryption, the mainstay of *asymmetric encryption* is using public and private keys. The *private key* is kept secret by one party during two-way encryption. Because the private key is never shared, its security is relatively maintained. The asymmetric key exchange process is therefore easier and more secure than the symmetric process.

The *public key* is given to anyone. Depending on the application of the encryption, either party may use the encryption key. The other key in the pair is used to decrypt. The private key in a pair can decrypt data encoded with the corresponding public key.

Asymmetric algorithms usually perform much slower than symmetric algorithms due to their larger key sizes.

Asymmetric Encryption Techniques

We lead

- RSA
- DH
- ECC
- DHE
- ECDHE

Rivest Shamir Adleman

Asymmetric Encryption Techniques

UMT
We lead

Asymmetric Algorithm	Description
Rivest Shamir Adelman (RSA)	Named for its designers, Ronald Rivest, Adi Shamir, and Len Adelman, RSA was the first successful algorithm for public key encryption. It has a variable key length and block size. It is still widely used and considered highly secure if it employs sufficiently long keys.
Diffie-Hellman (DH)	A cryptographic technique that provides for secure key exchange. Described in 1976, it formed the basis for most public key encryption implementations, including RSA, DHE, and ECDHE.
Elliptic curve cryptography (ECC)	An asymmetric, public key encryption technique that leverages the algebraic structures of elliptic curves over finite fields. ECC is used with wireless and mobile devices.
Diffie-Hellman Ephemeral (DHE)	A variant of DH that uses ephemeral keys to provide secure key exchange.
Elliptic Curve Diffie-Hellman Ephemeral (ECDHE)	A variant of DH that incorporates the use of ECC and ephemeral keys.

RSA Algorithm

UMT
We lead

Ron **Rivest**, Adi **Shamir**, and Len **Adleman** have developed this algorithm (**Rivest-Shamir Adleman**). It is a block cipher that converts plain text into ciphertext and vice versa on the receiver side.

- **The algorithm works as follow:**

1. Select two prime numbers **p** and **q** where $p \neq q$.
2. Calculate $n = p * q$.
3. Calculate $\Phi(n) = (p-1) * (q-1)$. (**Φ = Phi**)
4. Select e such that, e is relatively prime to $\Phi(n)$
   i.e. $(e, \Phi(n)) = 1$ and $1 < \emptyset(n)$
5. Calculate $d = e^{-1} \bmod \emptyset(n)$ or $ed = 1 \bmod \Phi(n)$.
6. Public key = {e, n}, private key = {d, n}.
7. Find out Cipher text using the formula,
   $C = P^e \bmod n$
   Where, $P < n$ and
   C = Cipher text, P = Plain text, e = Encryption key and n = block size.
8. Find out Plain text using the formula,
   $P = C^d \bmod n$.
   Where, d = Decryption key.

RSA Algorithm

UMT
We lead

RSA Algorithm step by step explanation

Step – 1: Select two prime numbers p and q where $p \neq q$.

Step – 2: Calculate $n = p * q$.

Step – 3: Calculate $\Phi(n) = (p - 1) * (q - 1)$.

Step – 4: Select e such that, e is relatively prime to $\Phi(n)$.

i.e. $(e, \Phi(n)) = 1$ and $1 < e < \Phi(n)$

Step – 5: Calculate $d = e^{-1} \bmod \Phi(n)$ or $ed = 1 \bmod \Phi(n)$.

Step – 6: Public key = {e, n}, Private key = {d, n}.

Step – 7: Find out cipher text using the formula,

$CT = PT^e \bmod n$.

Where, $P < n$.

CT = Cipher text, PT = Plain text, e = Encryption key and n = block size.

Step – 8: Find out Plain text using the formula,

$PT = CT^d \bmod n$.

Where, d = decryption key.

RSA Algorithm

UMT
We lead

Explanation with example:

Step – 1: Two prime numbers p = 13, q = 11.

Step – 2: n = p * q = 13 * 11 = 143.

Step – 3: Φ (n) = (13 – 1) * (11 – 1) = 12 * 10 = 120.

Step – 4: Select e = 13, GCD (13, 120) = 1.

Step – 5:

Finding d:

- e * d mod Φ (n) = 1
- 13 * d mod 120 = 1

(**How to find:** d * e = 1 mod Φ (n) ➔ d = ((Φ (n) * i) + 1)/e

d = (120 + 1)/13 = 9.30 (∵ i = 1)

d = (240 + 1)/13 = 18.53 (∵ i = 2)

d = (360 + 1)/13 = 27.76 (∵ i = 3)

d = (480 + 1)/ 13 = 37 (∵ i = 4), (We have to stop finding d when we get the exact integer value.)

Step – 6: Public key = {13, 143} and Private key = {37, 143}.

Step – 7: Encryption:

Plain text PT = 13. (Where, PT < n)

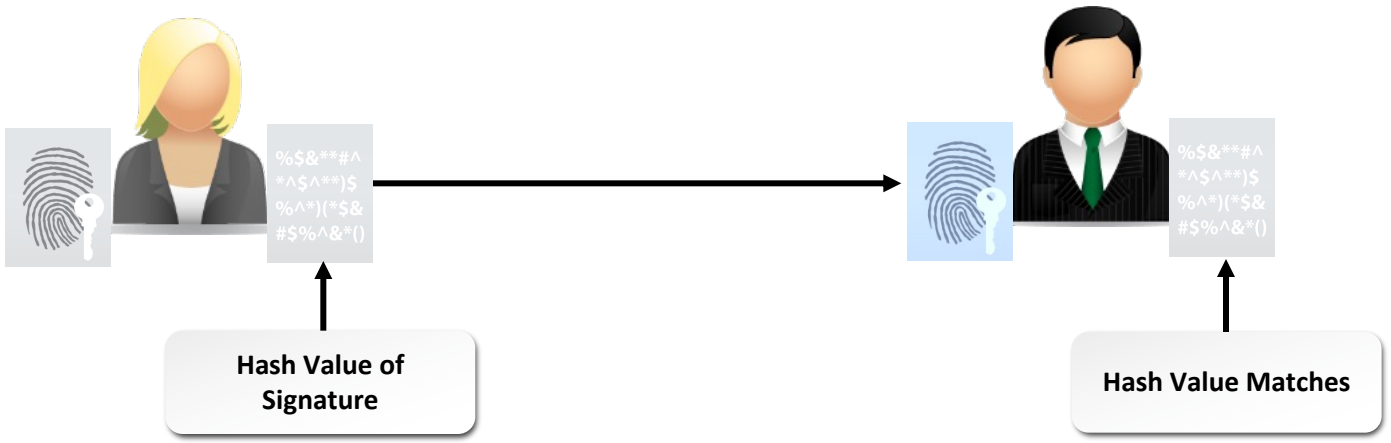
$CT = PT^e \bmod n$ ➔ $13^{13} \bmod 143$ ➔ 52, Then C = 52.

Step – 8: Decryption:

$P = CT^d \bmod n$ ➔ $52^{37} \bmod 143$ ➔ 13, Then P = 13.

Digital Signatures

A *digital signature* is a message digest that has been encrypted again with a user's private key. Asymmetric encryption algorithms can be used with hashing algorithms to create digital signatures.



Digital Signatures

UMT
We lead

Digital signature is a type of asymmetric cryptography used to simulate the security properties of a signature in digital, rather than written form

Digital signature schemes normally give two algorithms:

One for signing which involves the user's secret or private key (*Message Hash Algorithm*), and

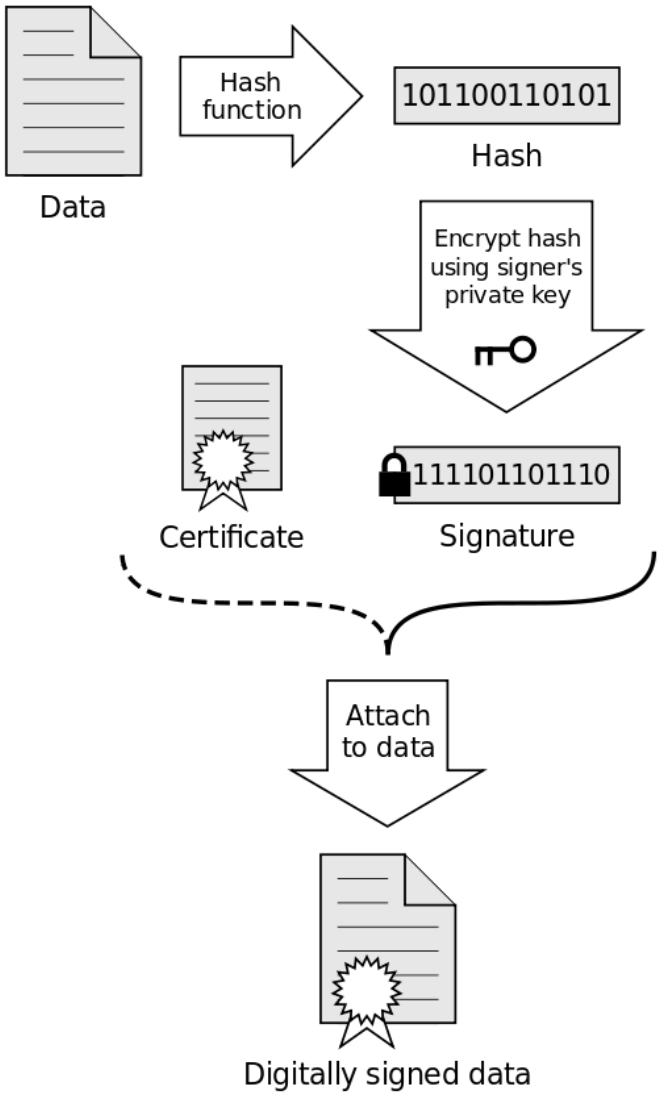
One for verifying signatures which involves the user's public key (*Public Key Encryption Algorithm*)

The output of the signature process is called the "digital signature"

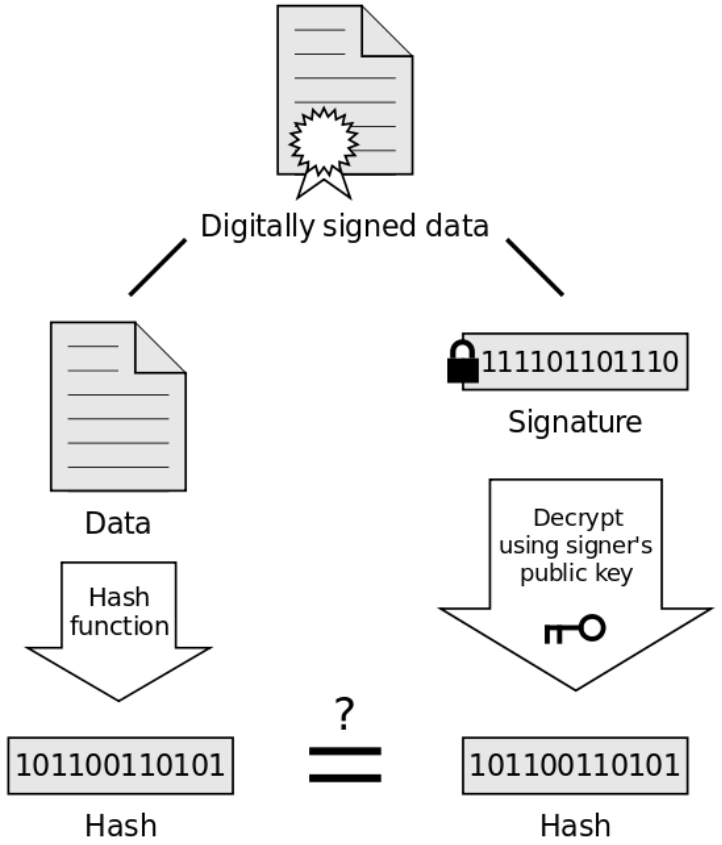
Digital Signatures

UMT
We lead

Signing



Verification



If the hashes are equal, the signature is valid.

Public Key Infrastructure (PKI)

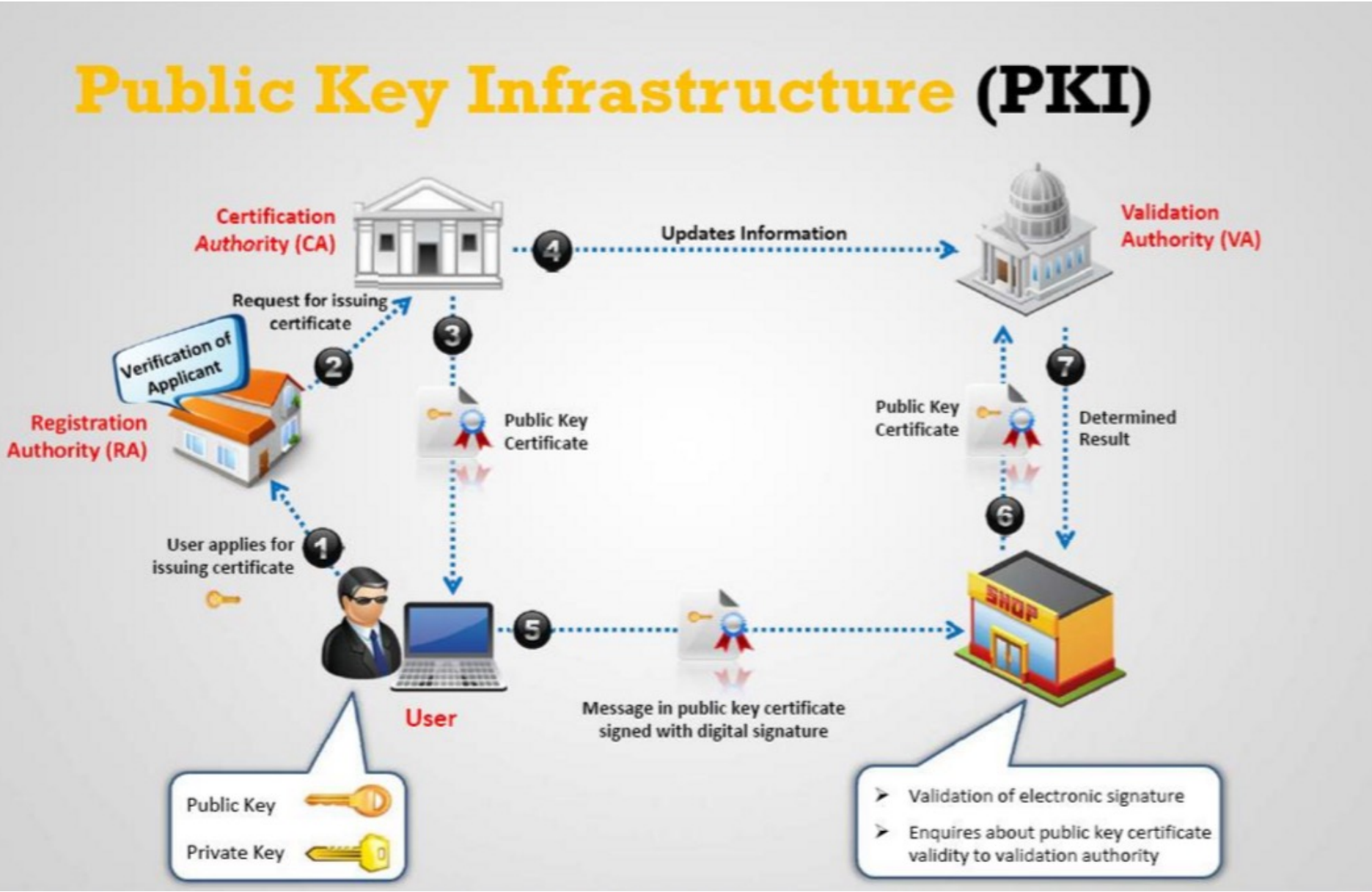
UMT
We lead

- A complete scheme for certifying bindings between public keys and identities— what key belongs to who— is called a Public Key Infrastructure (PKI)

- Necessary for widespread electronic commerce
- No absolute definition or standard

- A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of parties in Internet transactions

Public Key Infrastructure (PKI)

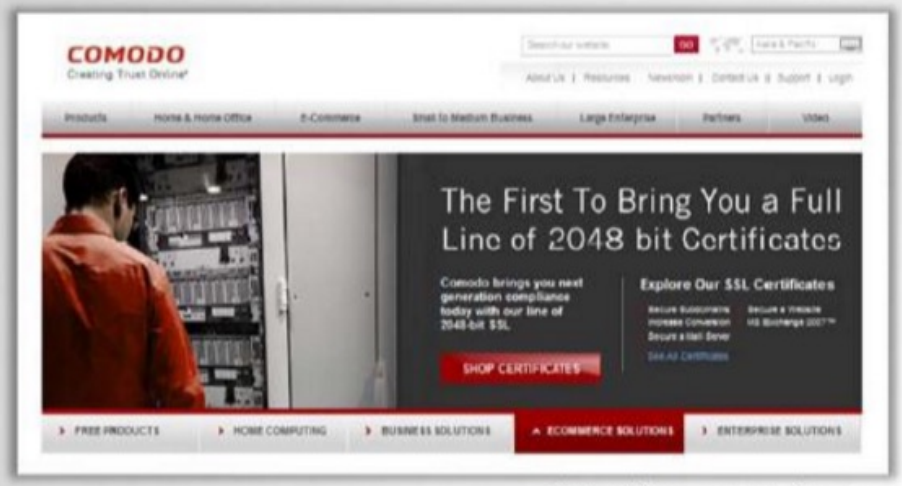


Public Key Infrastructure (PKI)

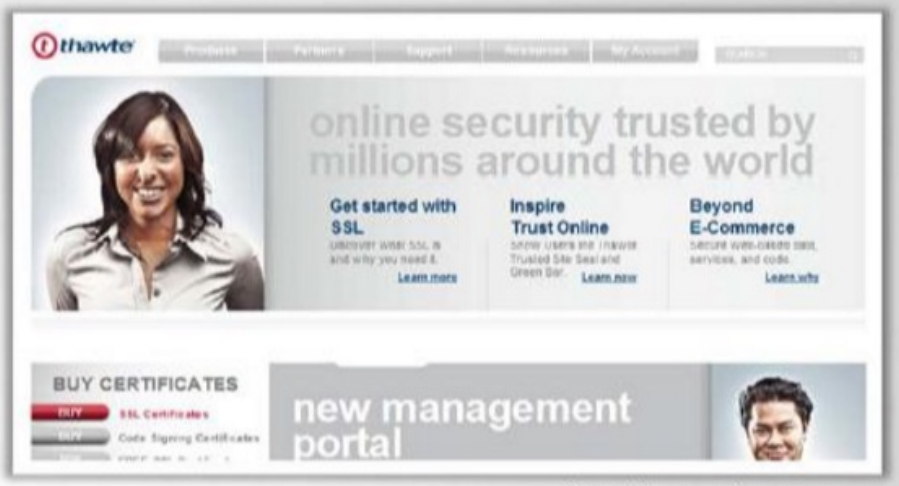
a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique within each CA domain. The third-party validation authority (VA) provide this information on behalf of CA. The binding is established through the registration and issuance process, which, depending on the assurance level of the binding, may be carried out by software at a CA or under human supervision. The PKI role that assures this binding is called the registration authority (RA), which ensures public key is *bound* to individual in a way that ensures non-repudiation. One of the major standards for certificates is known as X.509.

Certification Authorities

Certification Authorities

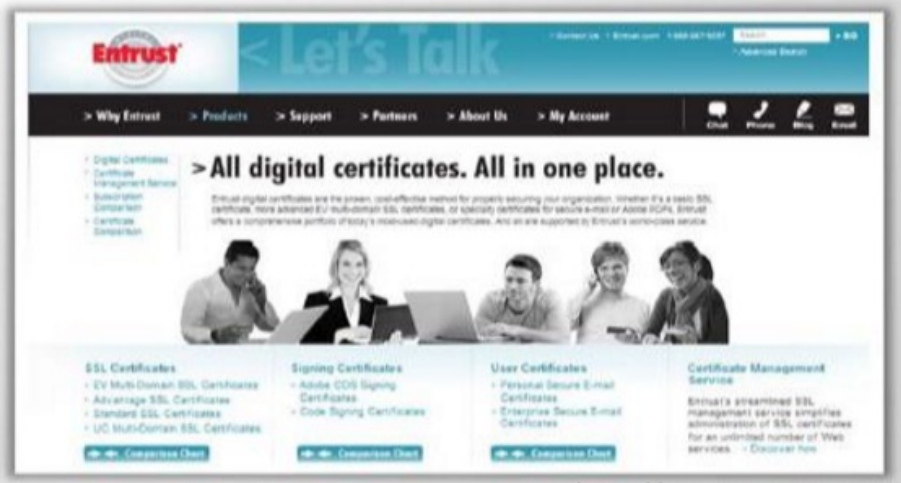


http://www.comodo.com



http://www.thawte.com

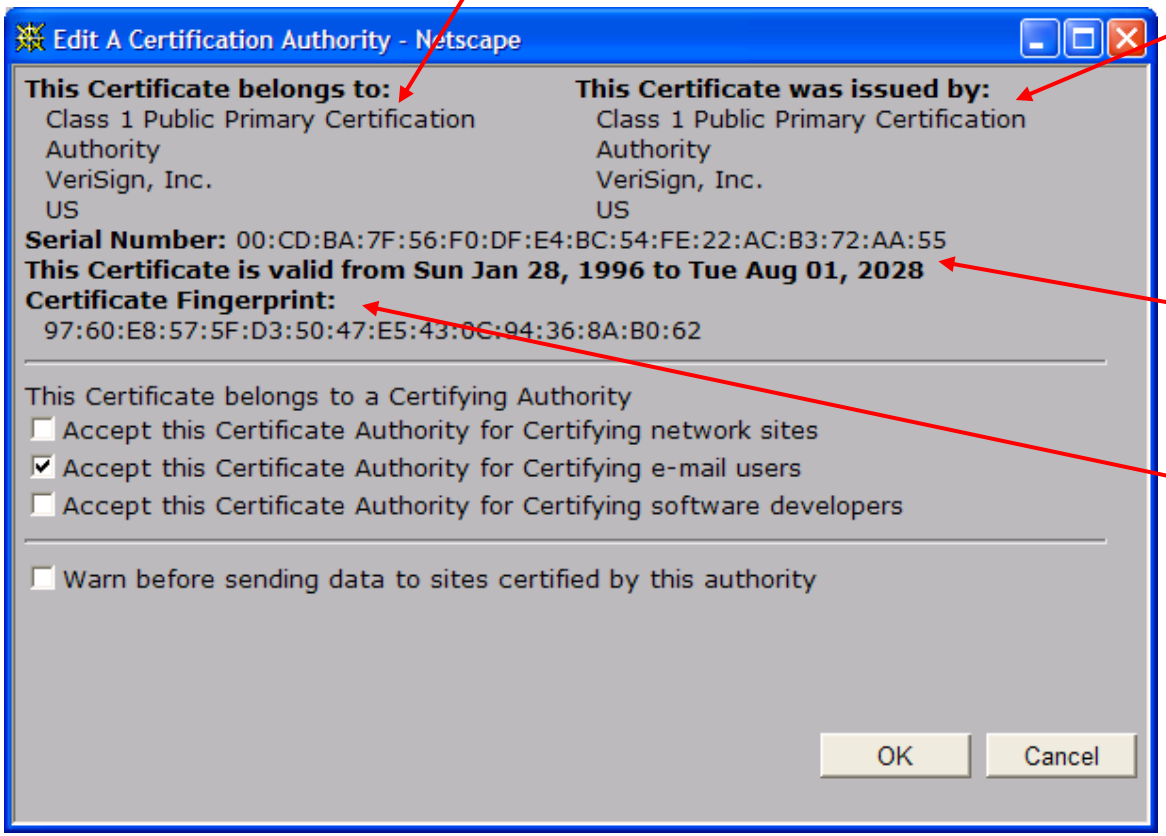
http://www.verisign.com



http://www.entrust.net

Certificate contains:

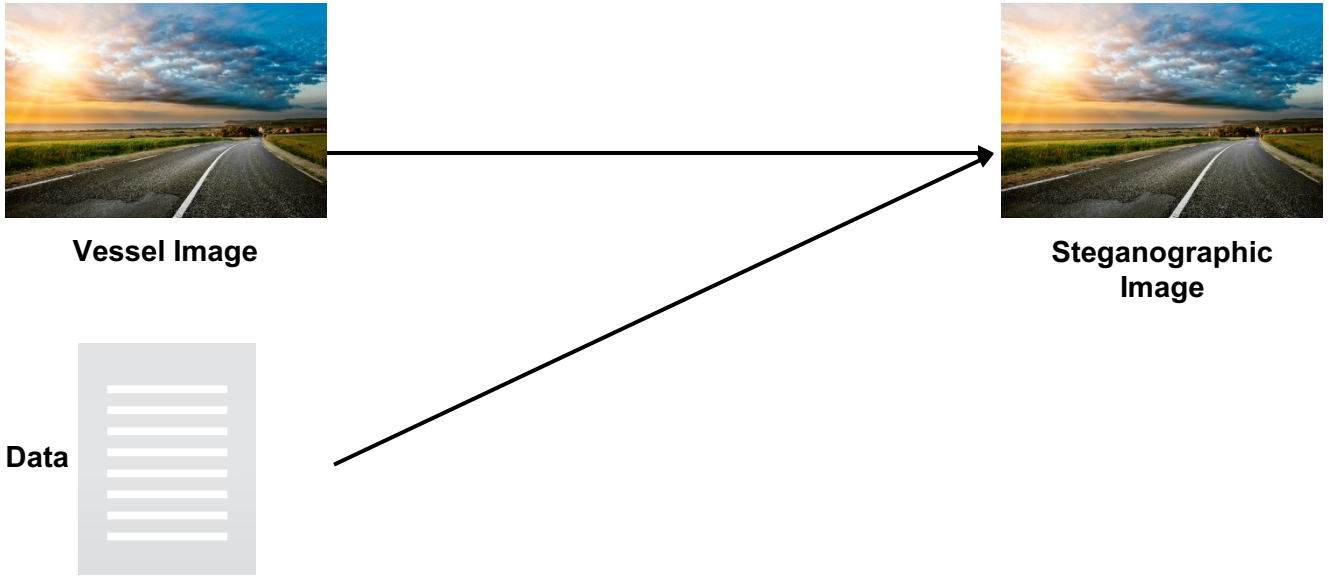
- Serial number (unique to issuer)
- info about certificate owner, including algorithm and key value itself (not shown)



- info about certificate issuer
- valid dates
- digital signature by issuer

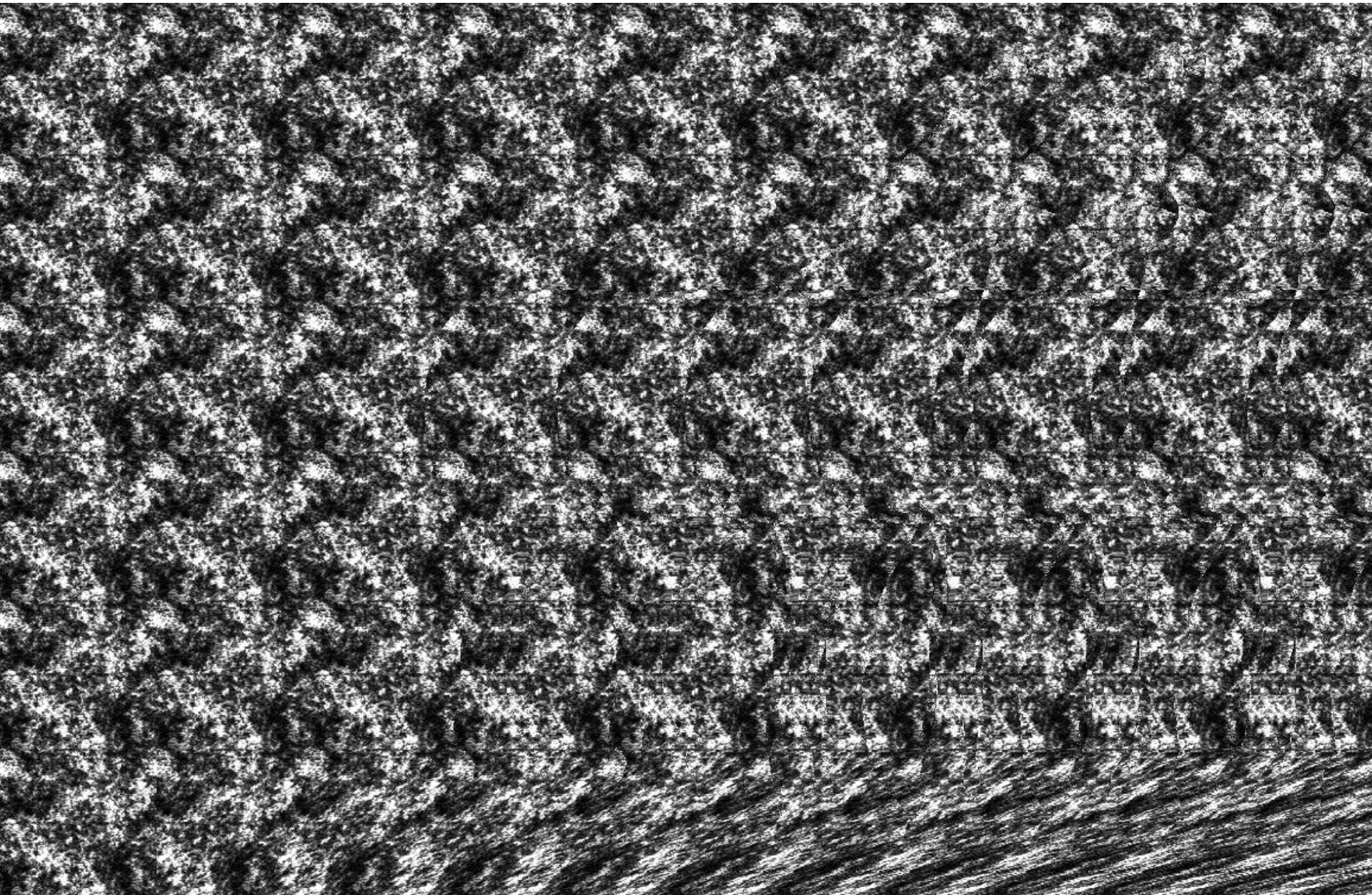
Steganography

- **Steganographic techniques include:**
  - Hiding information in blocks.
  - Hiding information within images.
  - Invisibly altering the structure of a digital image.



Steganography is an alternative cipher process that hides information by enclosing it in another file such as a graphic, movie, or sound file. Where encryption hides the content of information, but does not attempt to hide the fact that information exists, steganography is an attempt to obscure the fact that information is even present. Steganographic techniques include hiding information in blocks of what appears to be innocuous text, or hiding information within images either by using subtle clues, or by invisibly altering the structure of a digital image by applying an algorithm to change the color of individual pixels within the image.

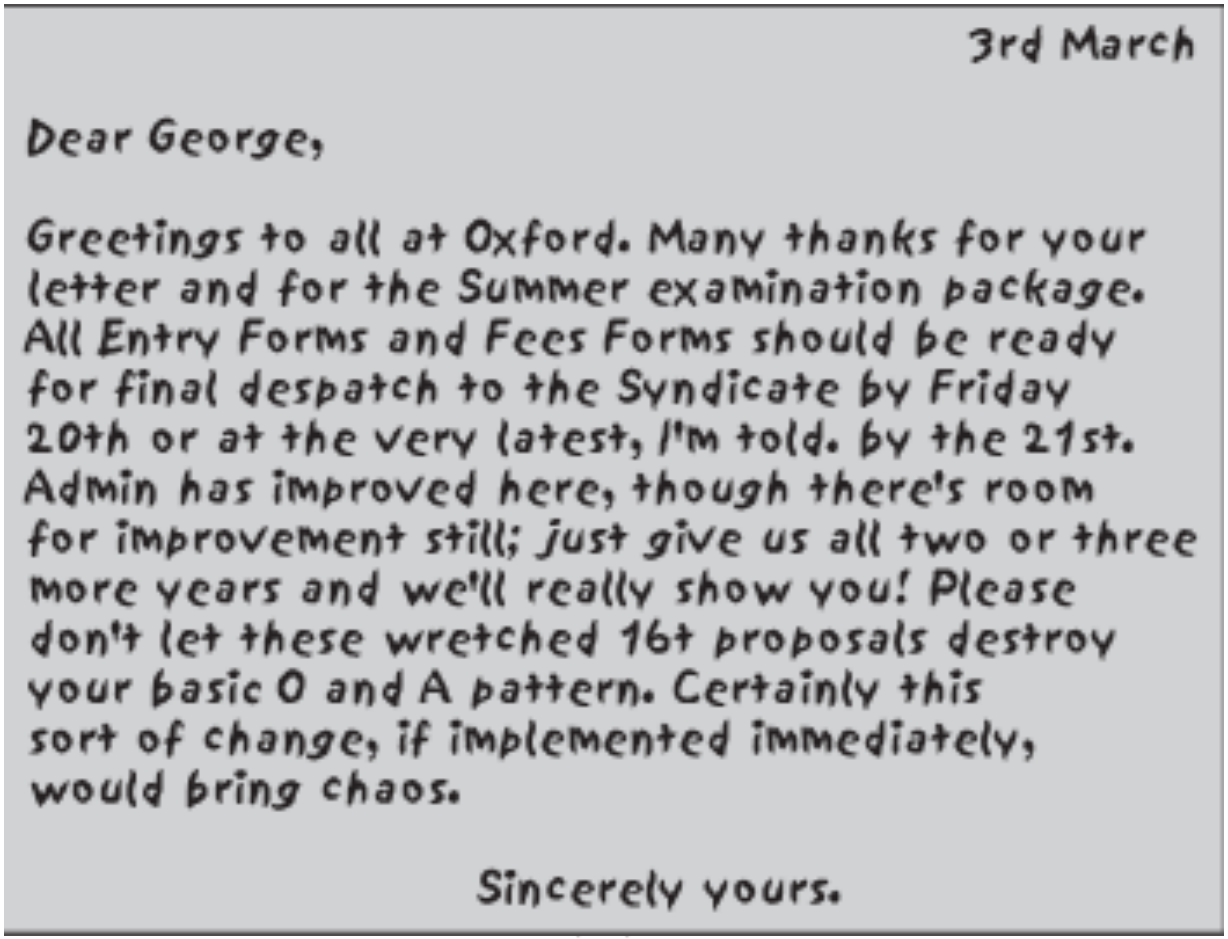
Steganography



Steganography

We lead

Example in which a subset of the words of the overall message is used to convey the hidden message. See if you can decipher this.



3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told. by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16t proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

Figure 2.9 A Puzzle for Inspector Morse
(from *The Silent World of Nicholas Quinn*, by Colin Dexter)

Word Steganography Example

Dear George,
Greetings to all at Oxford. Many thanks for **your** letter and for the summer examination **package**. All entry forms and fees forms should be **ready** for final dispatch to the syndicate by **Friday** 20th or at the latest I am told by the **21st**. Admin has improved here though there is **room** for improvement still; just give us all two or **three** more years and we will really show you! **Please** don't let these wretched 16+ proposals **destroy** your basic O and A pattern. Certainly **this** sort of change, if implemented **immediately**, would bring chaos.

Sincerely yours,

Other Steganography Techniques

- **Character marking**
  - Selected letters of printed or typewritten text are over-written in pencil
  - The marks are ordinarily not visible unless the paper is held at an angle to bright light
- **Invisible ink**
  - A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper
- **Pin punctures**
  - Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light
- **Typewriter correction ribbon**
  - Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light

Quotes

"Programming can be fun, so can cryptography; however they should not be combined."

- Kreitzberg and Shneiderman,
Authors

Thank you