Pre-Quantum Cryptology

Goutam Paul

Cryptology and Security Research Unit,
Indian Statistical Institute, Kolkata

February 9, 2016

Lecture at
International School and Conference on Quantum Information,
Institute of Physics (IOP), Bhubaneswar (Feb 9-18, 2016).

Cryptic Echos from Time Immemorial

Murmur of the Mummies

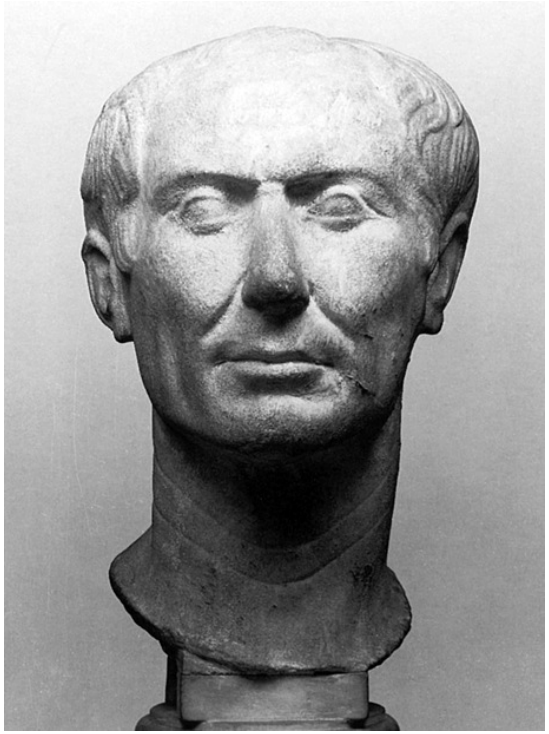
Egypt, 1900 BC:
Hieroglyph

Spirit of the Spartans

Greece, 700 BC: Scytale

Glories of the Gladiators

Julius Caesar, 100-44 B.C.:
Caesar Cipher

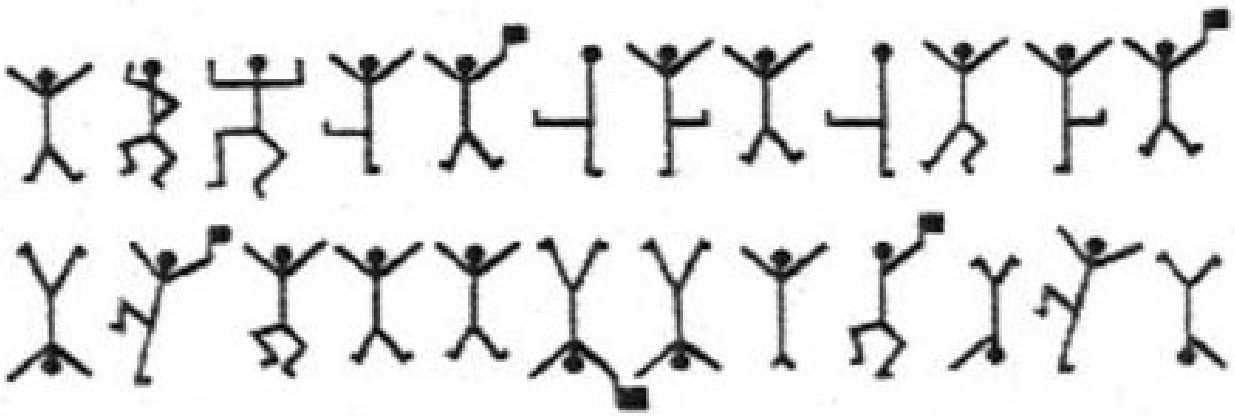


A French Saga

France, 1791-92 A.D.: Love letters sent by the Queen Marie-Antoinette to Count Axel von Fersen

Fiction I

Sir Arthur Conan Doyle, 1903:
The Adventure of the Dancing Men
(one of the Sherlock Holmes short stories).



Fiction II

Dan Brown, 2003: The Da Vinci Code (Cryptex)

Just before 2nd World War

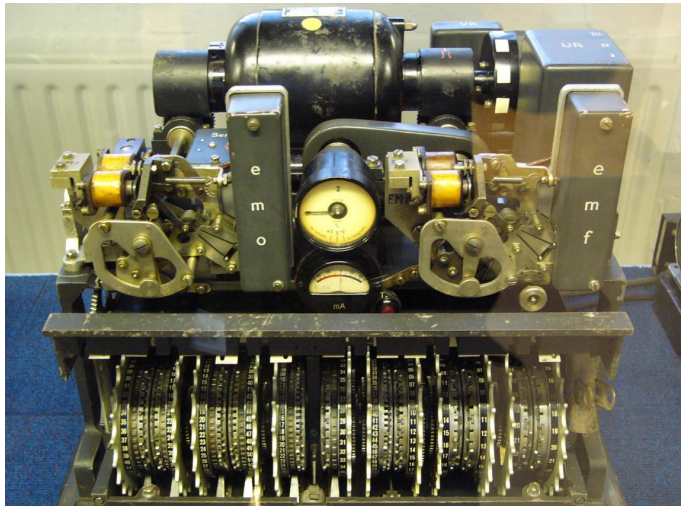
Germany, 1920 AD: Enigma

- Rotor machine with a keyboard, 3 scramblers, a reflector and a lamp-board, contained in 34 cm x 28 cm x 15 cm box weighing 12 kg
- Americans, French and British failed to break
- 1932: Broken by the Polish [Marian Rejewski]
- 1939: Handed over to the British

During 2nd World War

Germany, 1940 AD: Lorenz

- Used for high level German Army communications
- Had a metal base of 48 cm 39 cm x 43 cm
- Generated a pseudo-random character stream that was XOR-ed with the input characters to form the output characters
- Broken by British Mathematician William Tutte



After 2nd World War

- In Late '80s Cuban aircrafts attacked SA forces stationed in Namibia, killing many of their officers.
- They used *man-in-the-middle* attack.

Cryptology of Modern Times

Modern Cryptology

- Attributed to Claude Shannon, the father of mathematical cryptography.
- Shannon's seminal paper:
  Communication Theory of Secrecy Systems, in the Bell System Technical Journal, 1949.

Current Applications

- Online Credit card transactions
- Bank ATM connectivity and real time data transfer
- Instant Mobile recharge – US/Europe (Companies in India still use non-secure methods)
- Pre-paid electricity coupons – South Africa
- Pay TV-channel

State-of-the-Art

2012 AD, World Scenario

- At least 25 *very strong* research groups
- Around 8-10 Conferences per year (tier 1 and 2)
- 8-10 Reputed journals in the field of cryptology
- More than 300 *good* publications per year

What is Cryptology?

Definition: General Perspective

$$\text{CRYPTOLOGY} = \underset{\text{(hidden)}}{\text{'KRYPTOS'}} + \underset{\text{(study)}}{\text{'LOGIA'}}$$

Definition: General Perspective

$$\text{CRYPTOLOGY} = \underset{\text{(hidden)}}{\text{'KRYPTOS'}} + \underset{\text{(study)}}{\text{'LOGIA'}}$$

Cryptology is

- the Study and Practice of hiding information
- the Science and Technology of Information Security

Definition: Broadened Horizon

$$\text{CRYPTOLOGY} = \underset{\text{[making code]}}{\text{Cryptography}} + \underset{\text{[breaking code]}}{\text{Cryptanalysis}}$$

Definition: Broadened Horizon

$$\text{Cryptology} = \underset{\text{[making code]}}{\text{Cryptography}} + \underset{\text{[breaking code]}}{\text{Cryptanalysis}}$$

Cryptography
- Confidentiality
- Data Integrity
- Authentication
- Non-Repudiation

Definition: Broadened Horizon

Cryptology =	Cryptography	+	Cryptanalysis
	[making code]		[breaking code]
Cryptography	Confidentiality		
	Data Integrity		
	Authentication		
	Non-Repudiation		
Cryptanalysis	Vulnerabilities		

Background Requirement

- One requires a *strong* background in Mathematics and Computer Science.
- Moreover, the subject has interaction with Electronics, Tele Communication and Physics.

Background Requirement

- One requires a *strong* background in Mathematics and Computer Science.
- Moreover, the subject has interaction with Electronics, Tele Communication and Physics.

BEWARE: In many books, research documents and internet sites, ad-hoc solutions to different cryptologic problems are available. One should be careful that science cannot be replaced by ad-hoc heuristics.

Confidentiality or Privacy

A Practical Scenario: Net-Banking

GOAL: Transfer money from SBI account to UBI account

A Practical Scenario: Net-Banking

GOAL: Transfer money from SBI account to UBI account

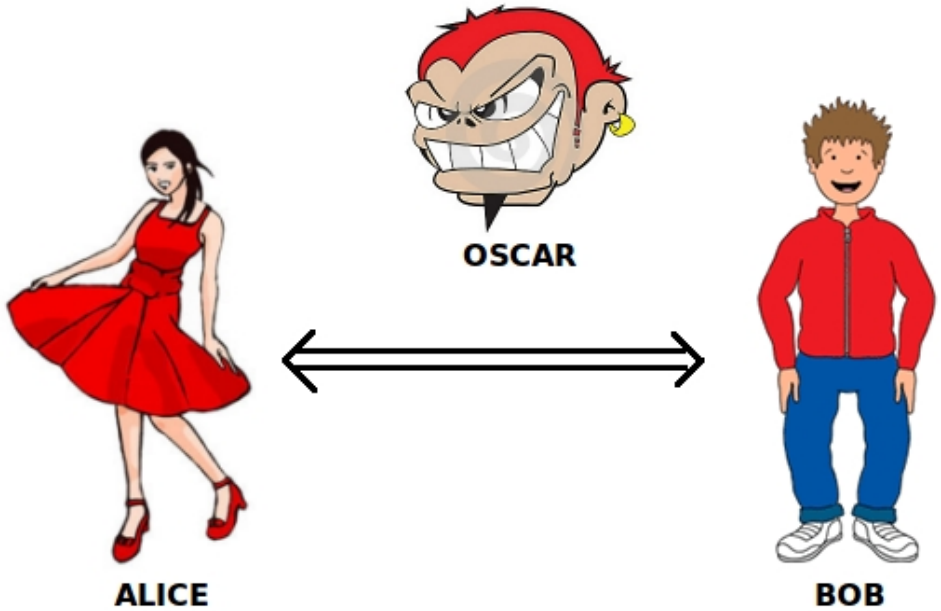
PROCEDURE

- Login to Net-Banking: Type your username and password.
- The password is communicated through internet (a public channel) from your computer to the SBI server.
- SBI server checks if the password is correct.
- If correct, SBI allows you to log in and make the transaction.

The Problem of Security

How will Alice and Bob communicate secretly?

(using a public channel where **Oscar** is eavesdropping)



Solution

- You need to communicate some modified (hidden) form of the password over the network.
- The SBI server will be able to transfer the modified form of the password to its proper form and check.
- Any other person will not be able to do the same.

Formal Model of a Cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$

- $\mathcal{P}$: a finite set of possible **plaintexts (messages)**.
- $\mathcal{C}$: a finite set of possible **ciphertexts**.
- $\mathcal{K}$ (**keyspace**): a finite set of possible keys.
- For each $K \in \mathcal{K}$ there exists
  - **encryption function** $e_K \in \mathcal{E}$ $(e_K : \mathcal{P} \to \mathcal{C})$ and a corresponding
  - **decryption function** $d_K \in \mathcal{D}$ $(d_K : \mathcal{C} \to \mathcal{P})$

  such that $d_K(e_K(x)) = x$ for every plaintext element $x \in \mathcal{P}$.

Cryptographic Attacks

Goal of Adversary

Secret disclosure

- Recover the Key(s) so as to break the secrecy

Distinguishing attack

- Distinguish the output of a cryptosystem from random generation

Malleability

- Transformations on the ciphertext to produce meaningful changes in the plaintext

Passive vs. Active Adversary

Passive vs. Active Adversary

- *Passive Adversary*: (S)he only monitors the communication channel.

Passive vs. Active Adversary

- *Passive Adversary*: (S)he only monitors the communication channel.
  Threatens confidentiality of data.

Passive vs. Active Adversary

- *Passive Adversary*: (S)he only monitors the communication channel.
  Threatens confidentiality of data.
- *Active Adversary*: (S)he attempts to alter or add or delete the transmissions over the channel.

Passive vs. Active Adversary

- *Passive Adversary*: (S)he only monitors the communication channel.
  Threatens confidentiality of data.
- *Active Adversary*: (S)he attempts to alter or add or delete the transmissions over the channel.
  Threatens data integrity and authentication also.

Attack Model I

Ciphertext only attack

The attacker knows certain ciphertext(s).

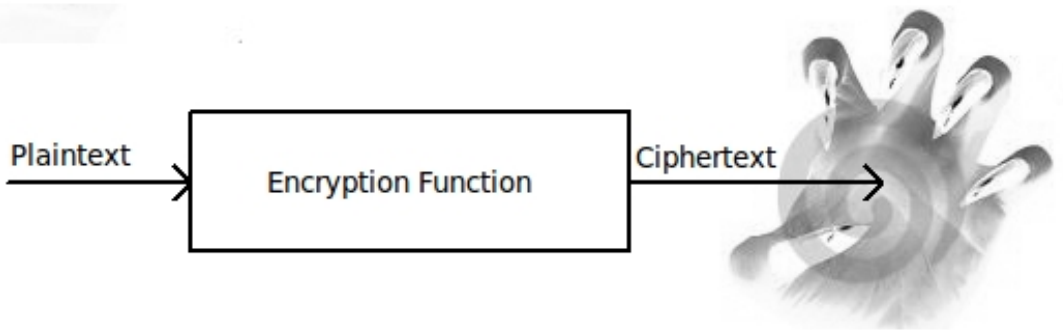


Figure : Ciphertext only attack

Target: To find message(s) and / or the key.

Attack Model II

Known plaintext attack

The attacker knows $(M_1, C_1), \ldots, (M_t, C_t)$.

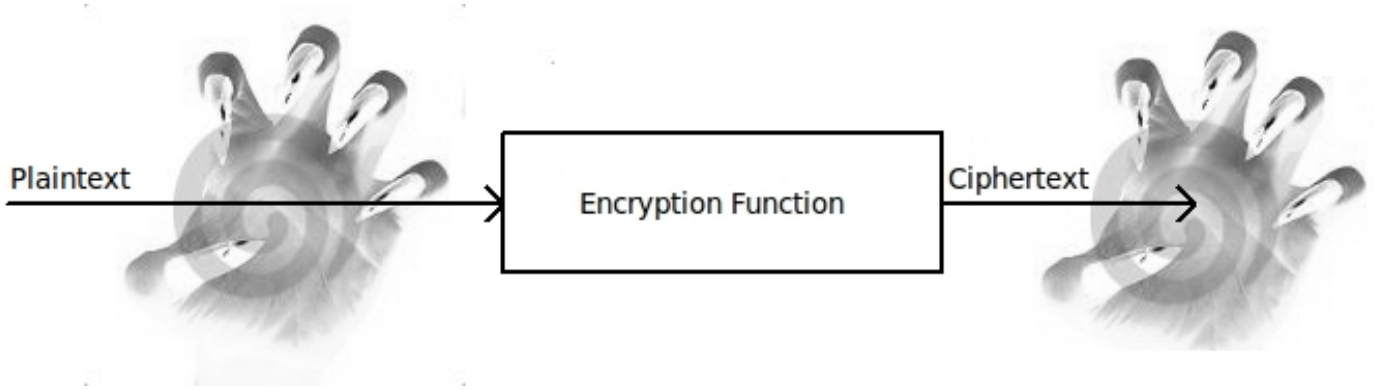


Figure : Known plaintext attack

Target: To find the key or a M^* corresponding to a new C^*.

Oracle

Oracle

An oracle is a **black box** that takes an input and gives an output (in almost no time).

Figure : An oracle is a **black box**.

Attack Model III

Chosen plaintext attack

The attacker chooses $M_1, \ldots, M_t$.
It receives corresponding $C_1, \ldots, C_t$.

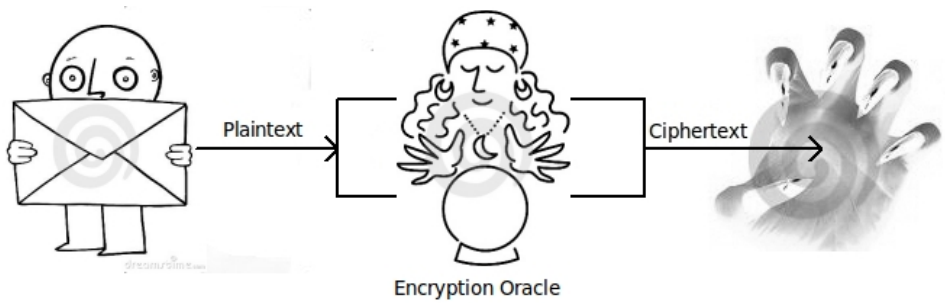


Figure : Chosen plaintext attack

Target: To find the key or a M^* corresponding to a new C^*.

Attack Model IV

Chosen ciphertext attack

The attacker chooses $C_1, \ldots, C_t$.
It receives corresponding $M_1, \ldots, M_t$.

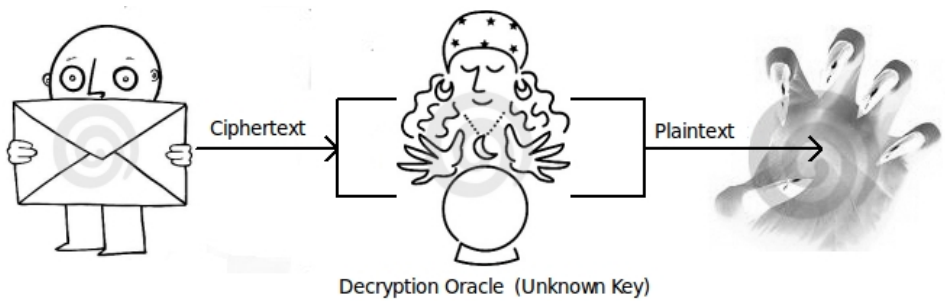


Figure : Chosen ciphertext attack

Target: To find the key or a M^* corresponding to a new C^*.

Cryptographic Security

Cryptographic Security

Cryptographic Security

- A. Kerckhoff (1883):
  The security of a cipher should rely on the secrecy of the key only!

Cryptographic Security

- A. Kerckhoff (1883):
  The security of a cipher should rely on the secrecy of the key only!
- Attacker knows every detail of the cryptographic algorithm except the key.

Rationale behind Kerckhoff's Principle

Rationale behind Kerckhoff's Principle

- Easy to maintain secrecy of a short key than to maintain secrecy of an algorithm.

Rationale behind Kerckhoff's Principle

- Easy to maintain secrecy of a short key than to maintain secrecy of an algorithm.
  Details of an algorithm can be leaked by an insider or may be reverse engineered.

Rationale behind Kerckhoff's Principle

- Easy to maintain secrecy of a short key than to maintain secrecy of an algorithm.
  Details of an algorithm can be leaked by an insider or may be reverse engineered.
- Easy to change a compromised key than to replace the algorithm / software used.

Rationale behind Kerckhoff's Principle

- Easy to maintain secrecy of a short key than to maintain secrecy of an algorithm.
  Details of an algorithm can be leaked by an insider or may be reverse engineered.
- Easy to change a compromised key than to replace the algorithm / software used.
  It is a good security practice to refresh the key even when it has not been exposed.

Rationale behind Kerckhoff's Principle

- Easy to maintain secrecy of a short key than to maintain secrecy of an algorithm.
  Details of an algorithm can be leaked by an insider or may be reverse engineered.
- Easy to change a compromised key than to replace the algorithm / software used.
  It is a good security practice to refresh the key even when it has not been exposed.
- For many pairs of communicating people, it is easier for everybody to use the same algorithm or program but different keys than for everyone to use a different program that depends on the party with whom (s)he is communicating.

Advantages of Open Cryptographic Design

Advantages of Open Cryptographic Design

- Our confidence in the security of the algorithm is much higher if it has been extensively studied (by experts other than the designers themselves) and no weakness have been found.

Advantages of Open Cryptographic Design

- Our confidence in the security of the algorithm is much higher if it has been extensively studied (by experts other than the designers themselves) and no weakness have been found.
- If a security flaw is found, that can be fixed.

Advantages of Open Cryptographic Design

- Our confidence in the security of the algorithm is much higher if it has been extensively studied (by experts other than the designers themselves) and no weakness have been found.
- If a security flaw is found, that can be fixed.
  For secret algorithm, the flaws may be known only to the malicious parties.

Advantages of Open Cryptographic Design

- Our confidence in the security of the algorithm is much higher if it has been extensively studied (by experts other than the designers themselves) and no weakness have been found.
- If a security flaw is found, that can be fixed.
  For secret algorithm, the flaws may be known only to the malicious parties.
- Public design enables the establishments of standards.

Security Models

Security Models

- *Unconditional Security* or *Perfect Secrecy*: The cryptosystem cannot be broken, even with infinite computational resources.

Security Models

- *Unconditional Security* or *Perfect Secrecy*: The cryptosystem cannot be broken, even with infinite computational resources.
- *Computational Security*: The best known algorithm for breaking the cryptosystem requires at least n operations, where n is some specified, very large number.

Security Models

- *Unconditional Security* or *Perfect Secrecy*: The cryptosystem cannot be broken, even with infinite computational resources.
- *Computational Security*: The best known algorithm for breaking the cryptosystem requires at least n operations, where n is some specified, very large number.
- *Provable Security*: The cryptosystem is as difficult to break as solving some well-known and supposedly hard problem.

Symmetric Key Cryptography

Basic Definition

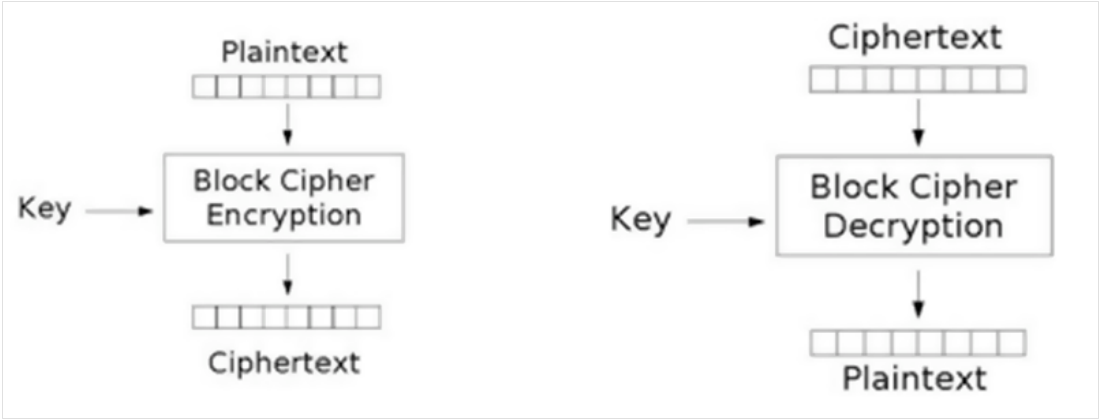
Symmetric Key

Identical keys used for encryption and decryption.

Figure : Same key is used to lock and unlock the chest.

Block Cipher

- The message is divided into fixed length group of bits (called **blocks**).
- Each block is encrypted with the same key.
- Encryption involves complicated mixing of the plaintext with the key.



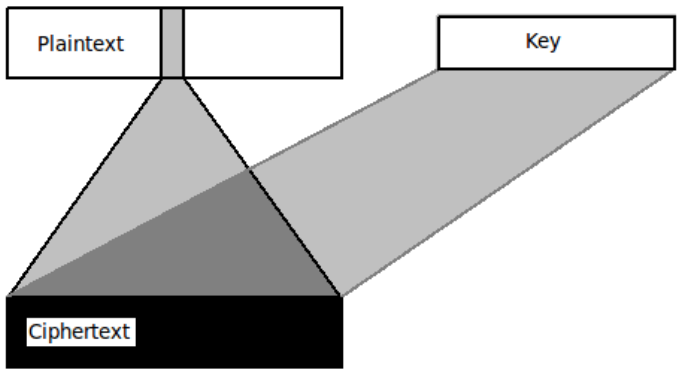
Block Cipher Design Criteria

Diffusion

The phenomenon of dissipation of redundancy in statistics of plaintext in the statistics of the ciphertext.

Confusion

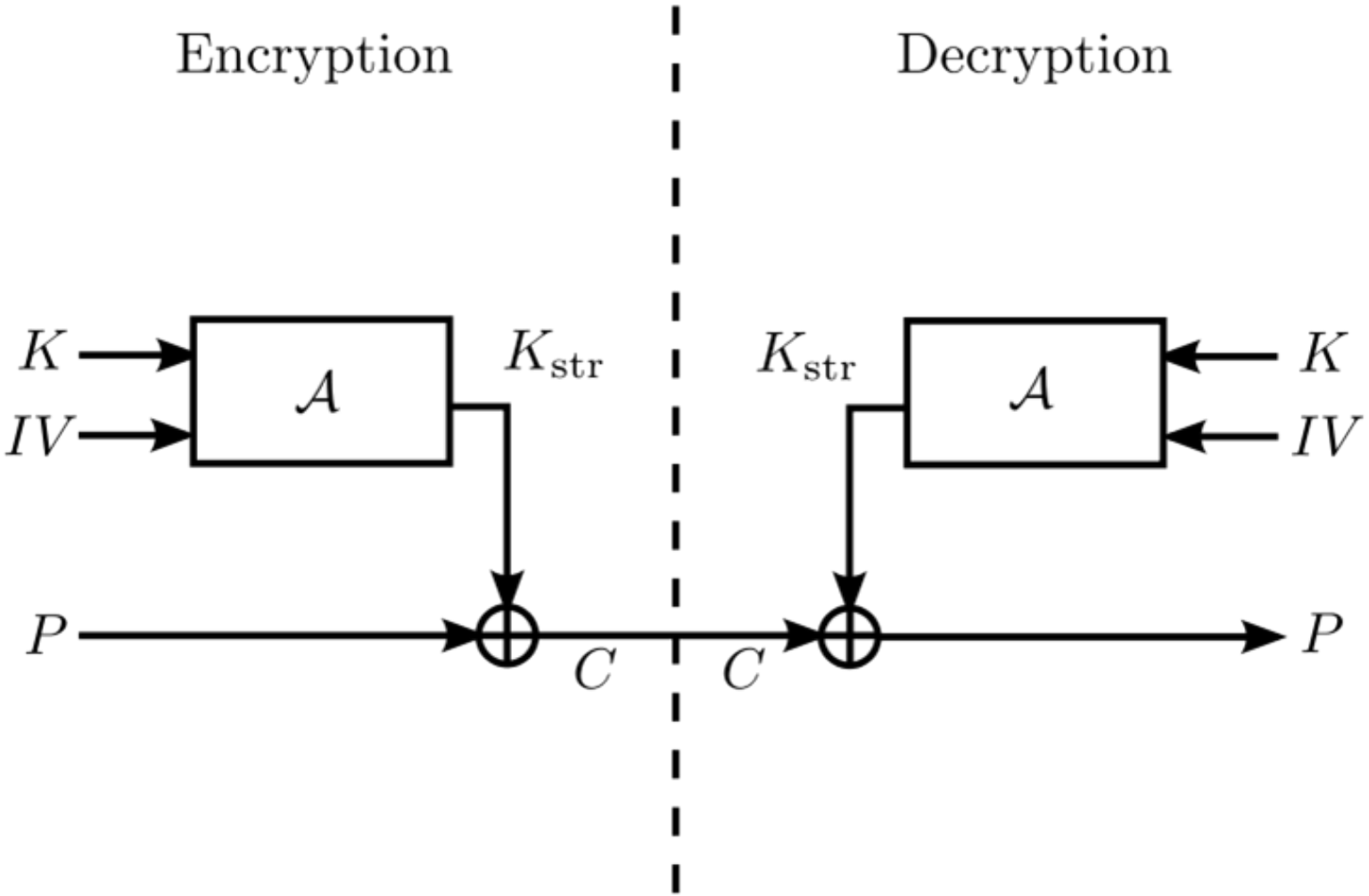
The phenomenon of making the statistical relationship between a key and its corresponding ciphertext as complex as possible.



Examples of Block Ciphers

- Shift Cipher
- Affine Cipher
- Vigenère Cipher
- Hill Cipher
- Permutation / Transposition Cipher
- Substitution Cipher
- DES
- AES

Stream Cipher



One Time Pad

One Time Pad

- A different keystream is used with each different plaintext message.

One Time Pad

- A different keystream is used with each different plaintext message.
- Has the property of perfect secrecy.

One Time Pad

- A different keystream is used with each different plaintext message.
- Has the property of perfect secrecy.
- Cannot be realized in practice (because of the FSM property).

How to generate a random stream in practice?

How to generate a random stream in practice?

- The best possible method of generating K_i's:

How to generate a random stream in practice?

- The best possible method of generating K_i's: toss an "unbiased" coin.

How to generate a random stream in practice?

- The best possible method of generating K_i's: toss an "unbiased" coin.
  - practically not feasible, when the parties are far apart.

How to generate a random stream in practice?

- The best possible method of generating K_i's: toss an "unbiased" coin.
  - practically not feasible, when the parties are far apart.
- Pragmatic solution: a pseudo-random generator based on a common seed (called the *secret key*).

Issues with Symmetric Key

Advantages

- Very very fast implementations possible
- Security can be very high (e.g: One-Time Pad)

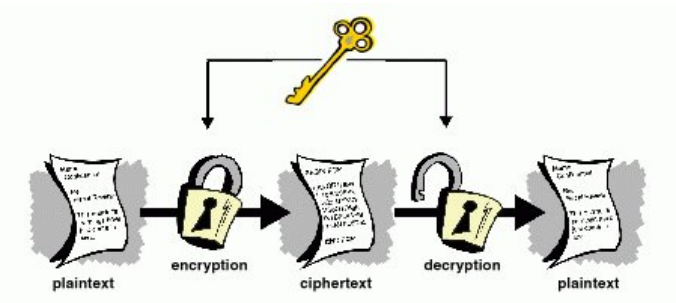
Disadvantages

- Secure key distribution is a major issue
- Hard to operate on a large distributed platform
- One participant compromised
  $\Longrightarrow$ Everything compromised

Public (Asymmetric) Key Cryptography

Symmetric vs. Asymmetric Key Cryptosystems

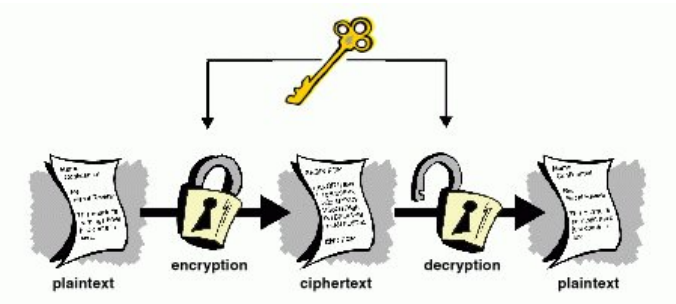
Symmetric Key



Same key for Bob & Alice

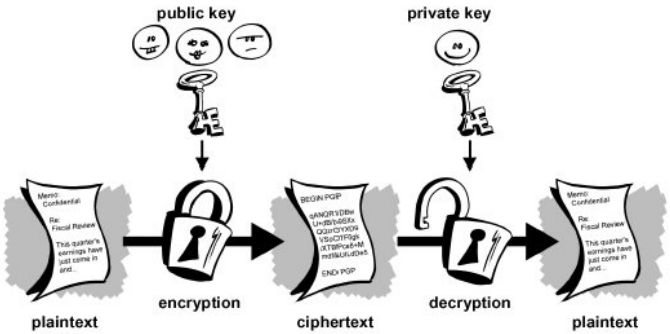
Symmetric vs. Asymmetric Key Cryptosystems

Symmetric Key



Same key for Bob & Alice

Asymmetric Key



Different keys for Bob & Alice

Origin and History

Timeline

- 1976: The Idea - Whitfield Diffie and Martin Hellman
- 1976: Diffie and Hellman Key Exchange algorithm
- 1978: Rivest, Shamir and Adleman invented RSA

Origin and History

Timeline

- 1976: The Idea - Whitfield Diffie and Martin Hellman
- 1976: Diffie and Hellman Key Exchange algorithm
- 1978: Rivest, Shamir and Adleman invented RSA

Actual Timeline (?) [announced in 1997]

- 1970: The Idea - James H. Ellis (British intelligence)
- 1973: Clifford Cocks developed RSA algorithm
- 1974: Malcom Williamson built Diffie-Hellman scheme

Public Key Framework

Goal: Alice and Bob communicate securely, avoiding Charles

Alice (receiver)	KEY GEN: Construct *related pair* of keys (public and private)
	KEY DIST: Publish public key and keep private key secret
Bob (sender)	GET KEY: Obtain an authentic Public Key of Alice
	ENCRYPT: Use it to encrypt message and send to Alice
Alice (receiver)	GET CIPHER: Obtain the ciphertext sent by Bob
	DECRYPT: Use Private Key to decrypt the ciphertext

Examples of Public Key Cryptosystems

- RSA
- ECC

Other Related Services

A few natural questions

- Is the data untampered?
- Is the data error-free?
- Can we rectify the data?
- Is the data unread?

Other Related Services

A few natural questions and their answers

- Is the data untampered? - Hash Functions
- Is the data error-free? - Checksums
- Can we rectify the data? - Error correcting codes
- Is the data unread? - Quantum tracing

Authentication and Integrity

Hash Functions

Hash function $H : \{0,1\}^* \rightarrow \{0,1\}^n$

Desirable properties

- Easy to compute the hash value for any given message
- Infeasible to find a message that has a given hash
- Infeasible to modify a message without changing its hash
- Infeasible to find two different messages having same hash

Origin of Digital Signatures

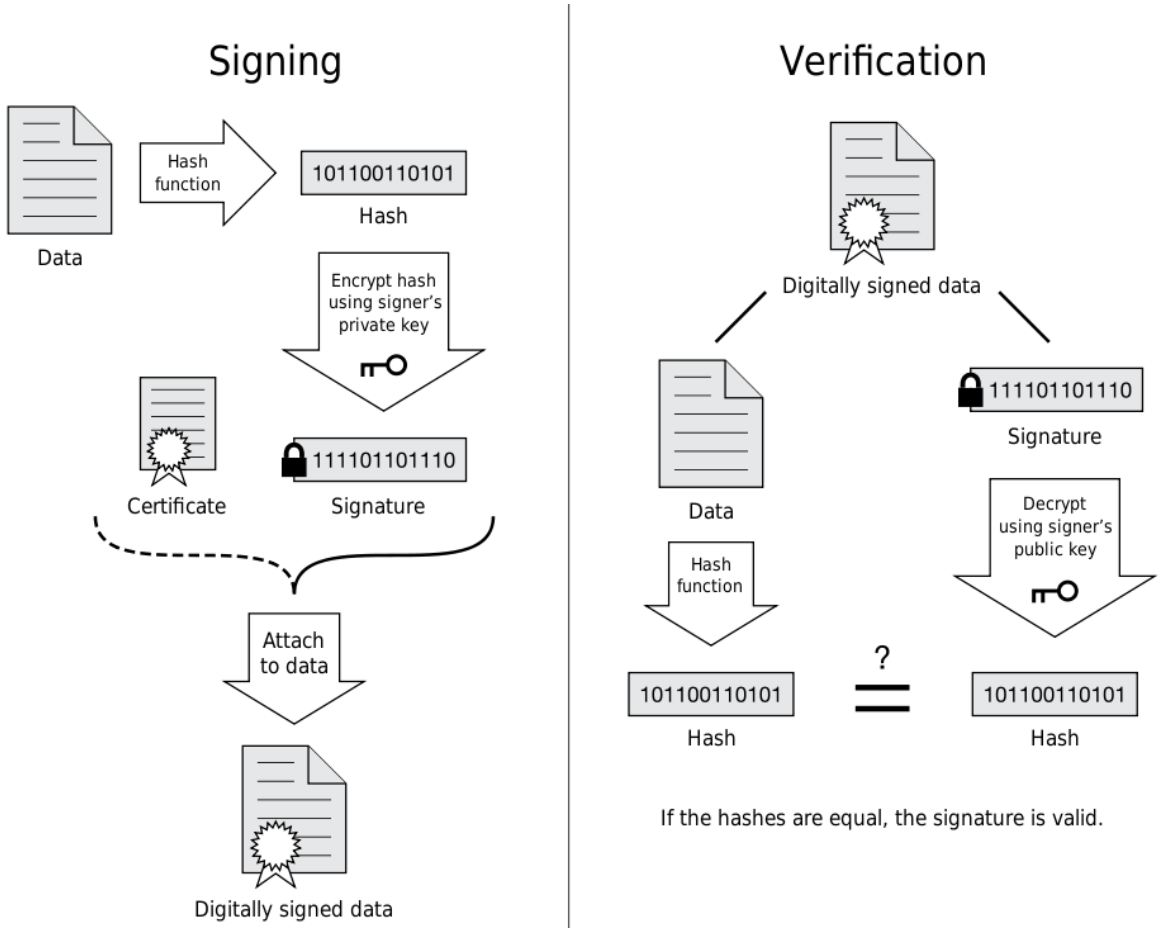
Origin

- 1976: Diffie and Hellman conjectured the idea
- 1978: RSA scheme provided a primitive

Famous Signature Schemes

- Full Domain Hash and RSA-PSS (based on RSA)
- Digital Signature Algorithm [DSA] and ECDSA
- El-Gamal Signature Scheme
- SHA-1, SHA-2 etc. (chosen by NIST)

An Outline of the Scheme



Non-Repudiation

Situation

- Alice sent Bob a message and signed it as well
- Bob went to George and claimed Alice sent the message
- George asked Alice and she *refused* straight away

Non-Repudiation

SITUATION

- Alice sent Bob a message and signed it as well
- Bob went to George and claimed Alice sent the message
- George asked Alice and she *refused* straight away

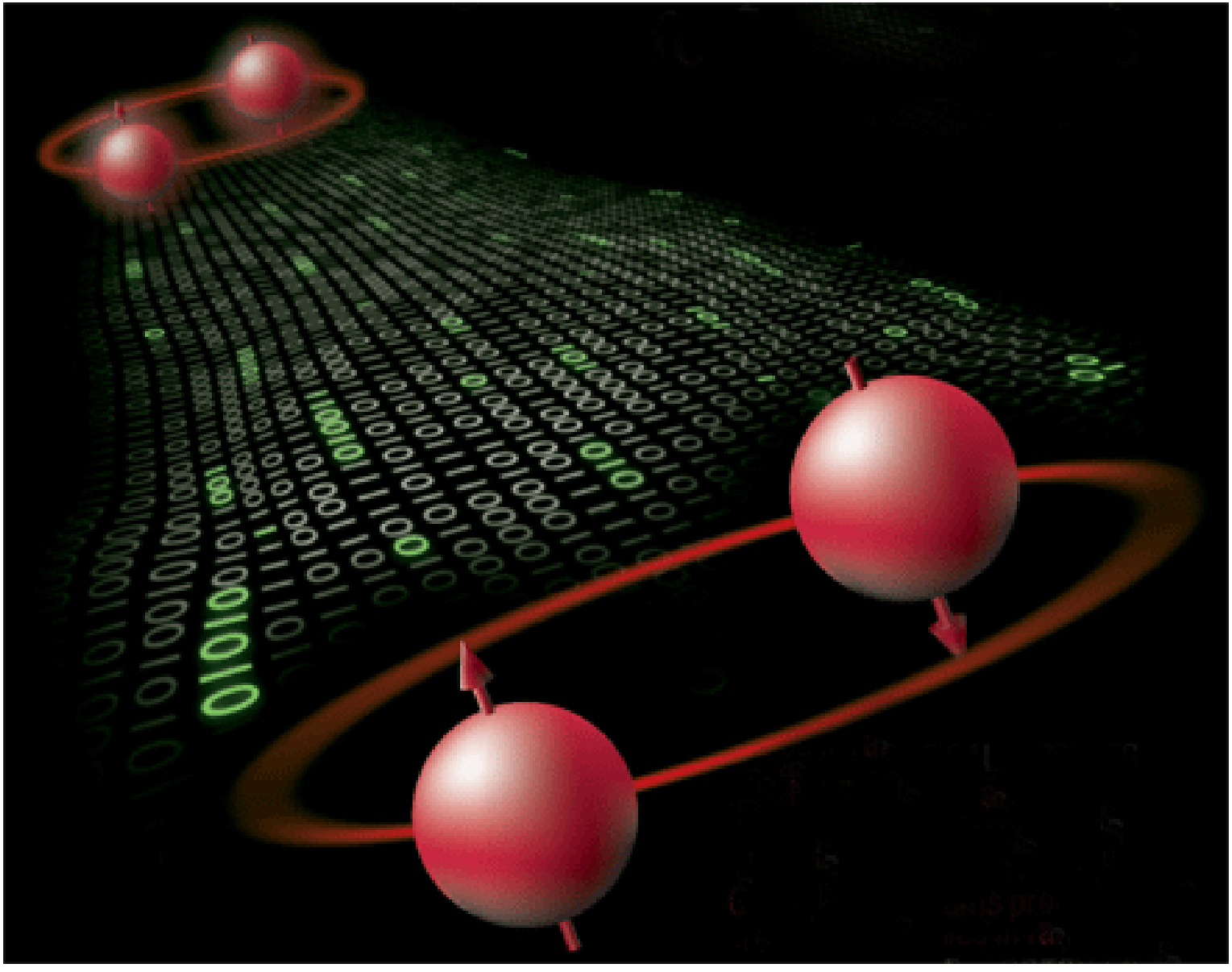
REPUDIATION: The denial of Alice as mentioned.
NON-REPUDIATION: Scheme to ensure this does not happen.

SOLUTION: Digital Signature using Private Key

Other Facets of Cryptology

- Identify Friend or Foe
- Key Establishment
- Secret Sharing
- Broadcast Encryption
- Zero-Knowledge Proof

Cryptology in the Quantum Era



Quantum World and Cryptology

- Data encoded by Photon Polarization, Electron Spin etc.
- State is a Mixture
- Measurement creates Collapse
- Entanglement
- Teleportation

Security and Cryptography

SITUATION: You have made all the transactions sitting on a computer at a cyber-cafe.

- Since you are typing the password on a third party machine, it is very easy to capture it by some background program.
- Thus even if you have a very strong cryptologic technique implemented, your password is leaked easily.

Security and Cryptography

SITUATION: You have made all the transactions sitting on a computer at a cyber-cafe.

- Since you are typing the password on a third party machine, it is very easy to capture it by some background program.
- Thus even if you have a very strong cryptologic technique implemented, your password is leaked easily.

SECURITY:
How to take care of these scientific/management problems?

Security and Cryptography

Lesson 1

You cannot have any security without cryptology.

Lesson 2

Even if you have implemented efficient and secured building blocks available from cryptography, you must need proper security management for actual implementation.

The Practical Scenario

- Most of the public domain cryptographic algorithms are free, no copyright or patent. You can implement them on your own and use.
- Every organization should have its own cryptography team. Buying a cryptosystem and using it blindly may pose serious problems. Better implement on your own and get it evaluated by different groups.
- Given a state-of-the-art cryptosystem, *complete break* is almost impossible. You need side channel information to get all/partial information.

Thank You

Questions / Comments ?

Homepage: http://www.goutampaul.com
Email: goutam.k.paul@gmail.com