Basics of Symmetric and Public Key Cryptography

Dr. Ashok Kumar Das

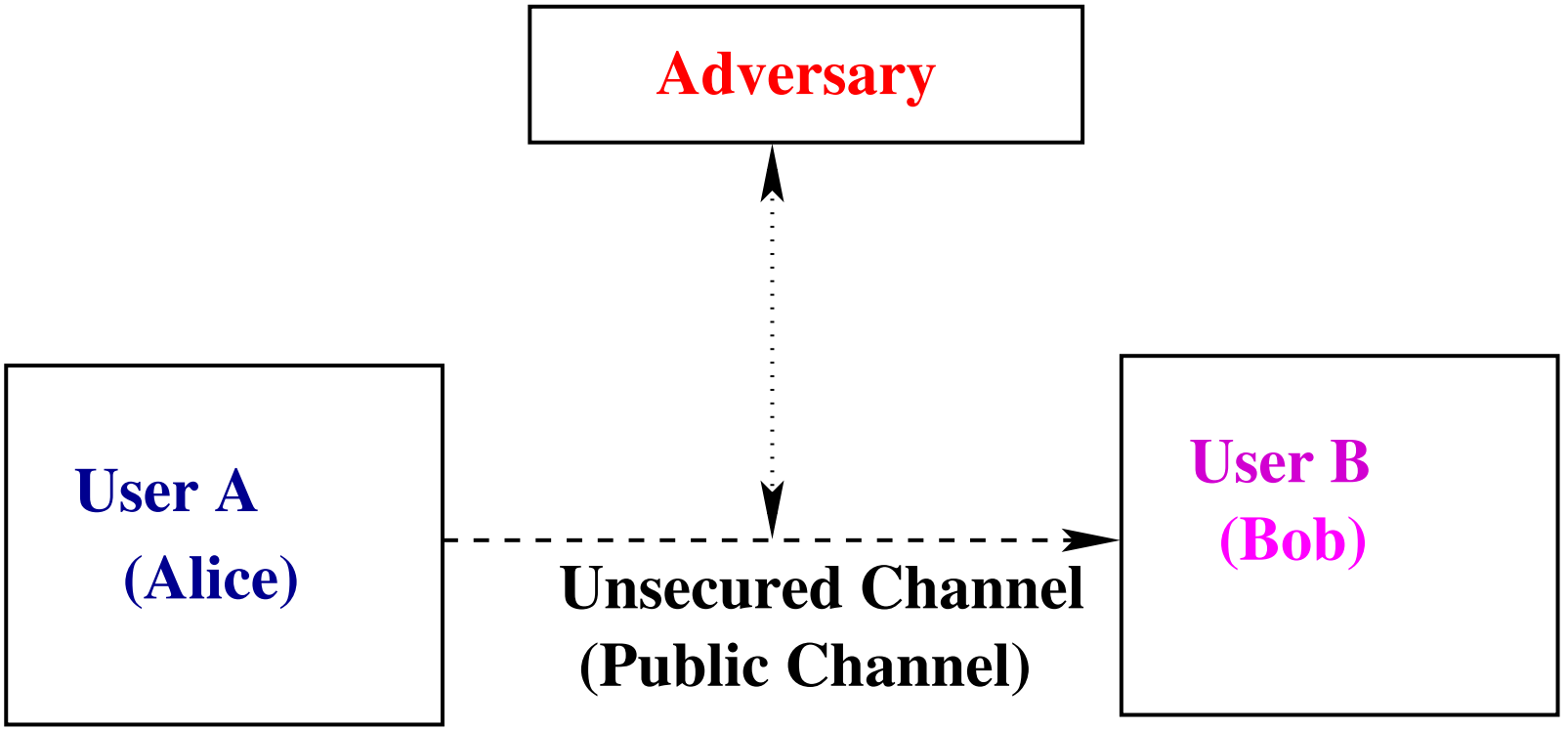
IEEE Senior Member
Professor
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad

E-mail: *ashok.das@iiit.ac.in*
URL: `http://www.iiit.ac.in/people/faculty/ashokkdas`
`https://sites.google.com/view/iitkgpakdas/`

What is Cryptography?

- Cryptography is the study of **mathematical techniques** related to aspects of information security such as confidentiality, data integrity, entity authentication, message authentication (data origin authentication) and non-repudiation.

Consider the following simple two-party communication model:



Introduction to Cryptography

- An "**adversary**" is an entity in a two-party communication which is neither the sender nor the receiver, and which tries to defeat the information security service being provided between the sender and the receiver.
- A "**channel**" is a means of conveying information from one entity to another entity.
- An "**unsecured (public) channel**" is one from which parties other than the sender and the receiver can reorder, delete, insert, or read the data being transmitted.
- A "**secured channel**" is one from which an adversary does not have the ability to reorder, delete, insert, or read the data being transmitted.

Types of adversary

- A "**passive adversary**" is an adversary who is only capable of reading information from an unsecured channel.
- An "**active adversary**" is an adversary who is capable to transmit, alter, or delete information on an unsecured channel.

Cryptographic goals (objectives)

- **Confidentiality:** Privacy (confidentiality) is a service of keeping information secret from all but those who are authorized to see it.
- **Data integrity:** ensuring information has not been altered by unauthorized or unknown means.
- **Entity authentication or identification:** Corroboration of the identity of an entity (i.e., a person, a computer terminal, a credit card, etc.).
- **Message or data origin authentication:** Corroborating the source of information.
- **Non-repudiation:** Preventing the denial of the previous session (preventing the malicious nodes to hide their activities).

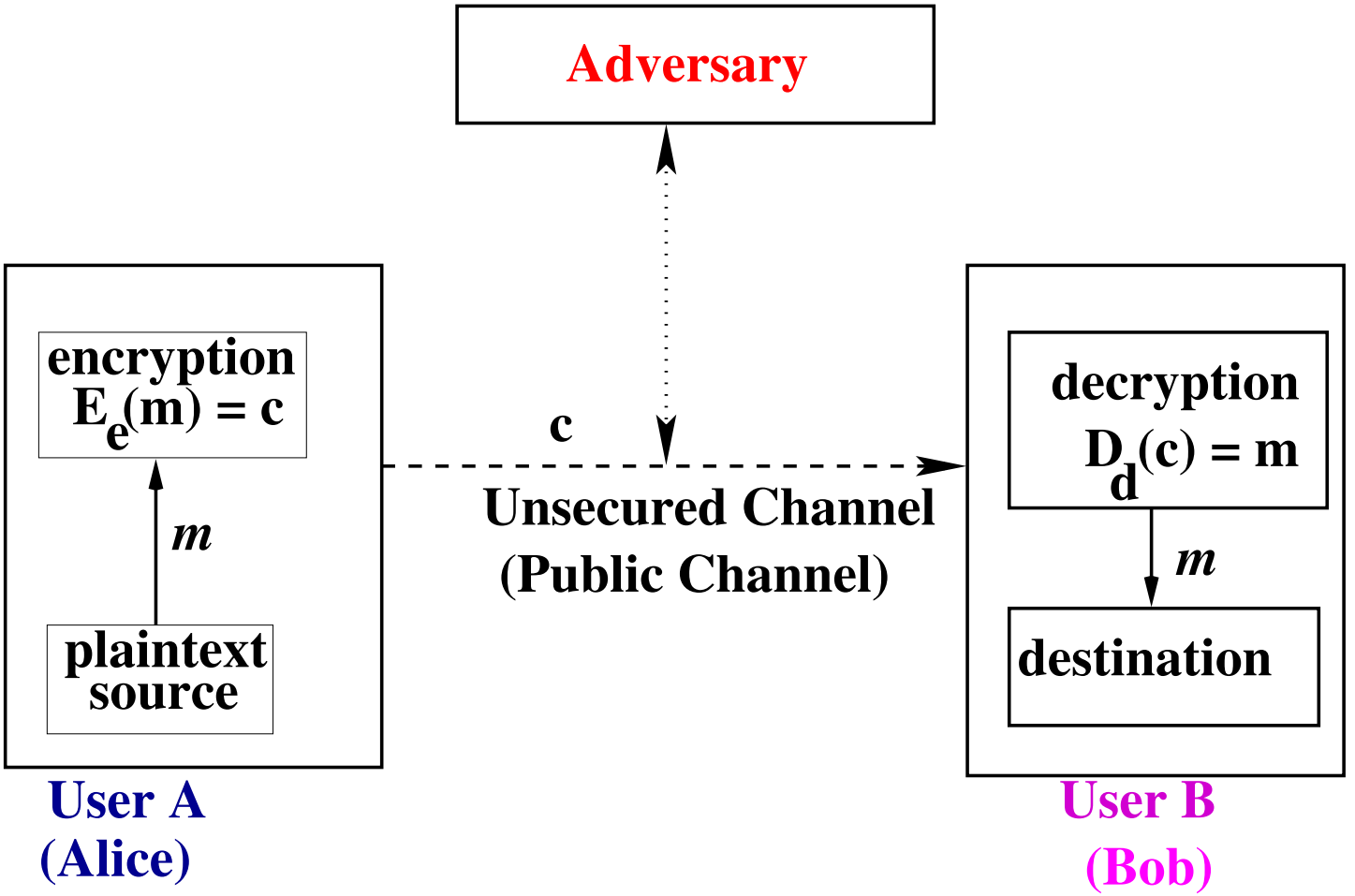
Cryptographic goals (objectives)

- **Authorization:** Conveyance to another entity such as a person or group of users. It ensures that the nodes (users) those who are authorized can be involved in providing information to network services.
- **Signature:** a means to bind information to an entity.
- **Access control:** restricting access to resources to privileged entity.
- **Certification:** endorsement of information by a trusted entity.

We need also to consider the forward and backward secrecy when new nodes join in the network and existing nodes depart from the network.

- ***Forward secrecy:*** When a node (user) leaves the network, it must not read any future messages after its departure.
- ***Backward secrecy:*** When a new node (user) joins in the network, it must not read any previously transmitted message.

Consider the following simple two-party communication model with encryption:



- **Security of the scheme**
  - Depends entirely on the secrecy of the key
  - Does not depend on the secrecy of the algorithm (Needs to be public for criticism!)
- Hence, we make the **assumptions** as follows:
  - Algorithms for encryption/decryption are known to the public
  - Keys used are kept secret

Definition

An encryption scheme (cipher or cryptosystem) is said to be ***breakable*** if a third party, without prior knowledge of the key pair (e, d), can systematically recover plaintext from corresponding ciphertext within some appropriate time frame.

Goal: We want this problem for an adversary (attacker) to be NP-hard (Computationally infeasible).

Definition (Brute-force attack)

An encryption scheme can be broken by trying all possible keys to see which one the communicating parties are using (assuming that the class of encryption functions is public knowledge).
This is called an exhaustive search of the key space.

What is meant by "Security lies in the keys" (using brute-force attack)

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

Symmetric-Key Encryption

Model of conventional (symmetric key) encryption

- Consider an encryption scheme consisting of
  - the set of encryption transformations $\{E_e : e \in K\}$
  - the set of corresponding decryption transformations $\{D_d : d \in K\}$, where K is the key space.
- The encryption scheme is said to be S-key or symmetric-key, if for each associated encryption/decryption key pair (e, d), it is computationally "easy" to determine d from e and to determine e from d.
- In most practical symmetric-key encryption schemes, $e = d$.
- Other terms used are single-key, one-key, private-key and conventional encryption.

Symmetric-Key Encryption

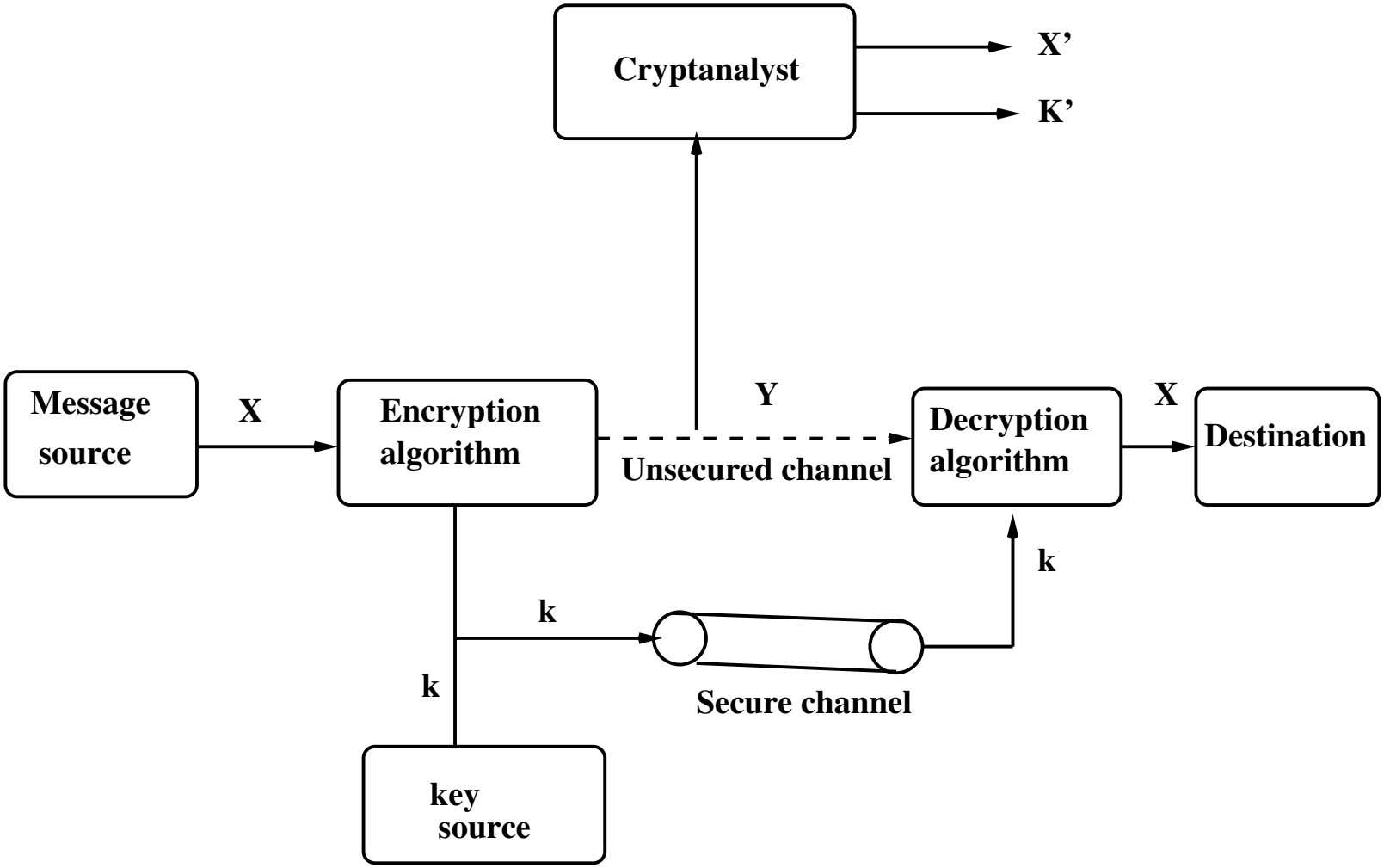


Figure: Model of conventional encryption

Symmetric-Key Encryption

Caesar Cipher

- It is the earliest known use of a substitution cipher, and the simplest, was by Julius Caesar.
- Each letter of the alphabet is replaced with the letter standing the three places further down the alphabet.
- For example,
  plaintext: meet me after the new year party
  ciphertext: PHHW PH DIWHU WKH QHZ BHDU SDUWB
- Each letter is wrapped around, so that the letter following Z is A. Define the transformation by listing all possibilities as follows.

plaintext:	a	b	c	...	v	w	x	y	z
ciphertext:	D	E	F	...	Y	Z	A	B	C

Caesar Cipher

- Encoding technique:
  Let us assign a numerical equivalent to each letter:

a	b	c	...	v	w	x	y	z
0	1	2	...	21	22	23	24	25

- Mathematical model:
  - Encryption: For each plaintext letter p, substitute the ciphertext letter c: $c = E_k(p) = (p + 3) \pmod{26}$, where $k = 3$.
  - Decryption: For each ciphertext letter c, substitute the plaintext letter p: $p = D_k(c) = (c - 3) \pmod{26}$, where $k = 3$.

The Generalized Caesar Cipher

- A shift may be of any amount, so that the general Caesar algorithm is as follows.
- Mathematical model
  - Encryption: For each plaintext letter p, substitute the ciphertext letter c: $c = E_k(p) = (p + k) \pmod{26}$, where $0 \leq k \leq 25$.
  - Decryption: For each ciphertext letter c, substitute the plaintext letter p: $p = D_k(c) = (c - k) \pmod{26}$, where $0 \leq k \leq 25$.

Security issues of the Caesar cipher

- If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed.
- The key space K in this case contains 25 keys, that is $|K| = 25$.
- Attacker simply tries all the 25 possible keys.
- In this case, the attacker could be able to recover the plaintext as well as the encryption key k from the ciphertext easily (It is an example of Ciphertext-only attack (COA)).

Symmetric-Key Encryption

Vernam Cipher

- An encryption system was introduced by an AT& T engineer named Gilbert Vernam in 1918.
- He introduced a new parameter (keyword) which is as long as the plaintext and has no statistical relationship to it.
- **Encryption algorithm**
  The system can be expressed as follows:
  $c_i = p_i \oplus k_i$
  where $p_i = i^{th}$ binary digit of plaintext,
  $c_i = i^{th}$ binary digit of ciphertext,
  $k_i = i^{th}$ binary digit of key,
  $\oplus =$ bitwise exclusive-or (XOR) operator.
- **Decryption algorithm**
  Because of the properties of XOR, decryption simply involves the same bitwise operation: $p_i = c_i \oplus k_i$.

Vernam Cipher

- **Construction of key:**
  - Keyword should be as long as the plaintext and can be repeating.
- Vernam cipher is an example of classical stream cipher.
- It is also called one-time pad, because each plaintext is appended with random key.
- It is proved in the literature that one-time pad is unbreakable (proof will be given mathematically later), since it produces random output that bears NO satistical relationship to the plaintext.

Symmetric-Key Encryption

Vernam Cipher

Problems with the one-time pad

- Generation of key.
- Problem of key distribution and protection.

Because of these difficulties, the one-time is of limited utility, and is used primarily for low-bandwidth channels requiring very high security.

Data Encryption Standard (DES)

- The most widely used encryption is based on the Data Encryption Standard (DES) adopted in 1977 by the National Institute of Standards and Technology (NIST), USA.
- For DES, data are encrypted in 64-bit blocks using a 56-bit key.
- The encryption algorithm transforms 64-bit input in a series of steps into a 64-bit output.
- The same steps, with the same key, are used to reverse the encryption (decryption).
- Mathematically, $DES : \{0,1\}^{64} \times \{0,1\}^{56} \longrightarrow \{0,1\}^{64}$ such that the ciphertext be $C = DES_K(P)$, where $K \in \{0,1\}^{56}$ is the 56-bit key, $P \in \{0,1\}^{64}$ is the plaintext message (block) and $C \in \{0,1\}^{64}$ is the ciphertext block.

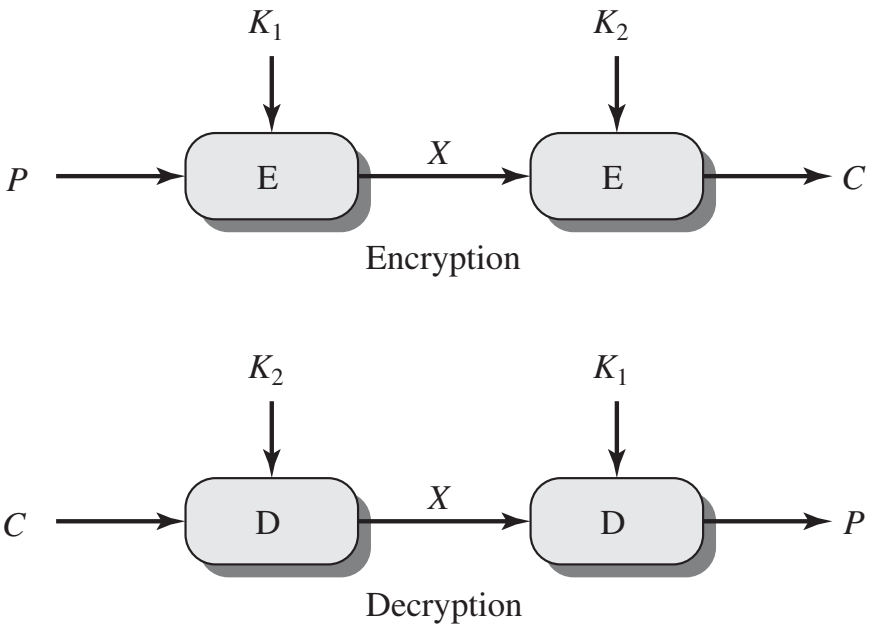
Symmetric-Key Encryption

Data Encryption Standard (DES)

- DES finally and definitely proved insecure in July 1998, when the Electronics Frontier Foundation (EFF) announced that it had broken a DES encryption using a special-purpose “DES cracker” machine that was built for less than 250,000 USD.
- The attack took less than three days.

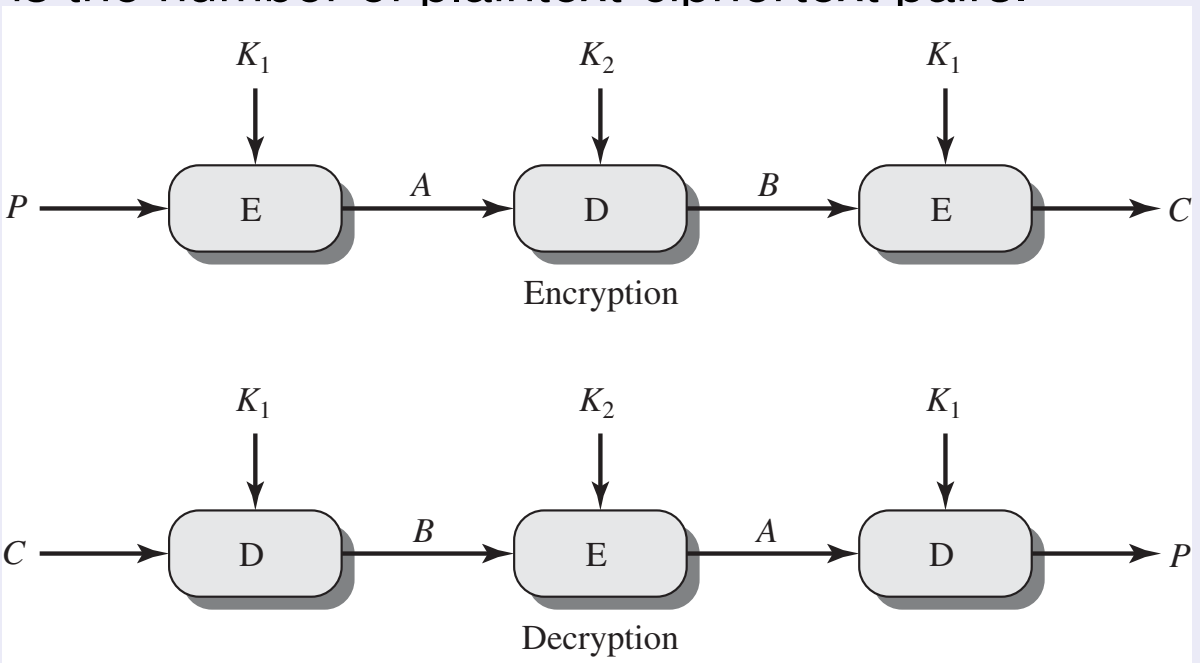
Double DES (2DES)

- It uses two 56-bit keys K_1 and K_2, and 64-bit plaintext block.
- It produces 64-bit ciphertext block.
- Known-plaintext attack (meet-in-the-middle attack) is possible against 2DES to derive two keys K_1 and K_2, which has a key size of 112 bits and with an effort on the order of 2^{56}.

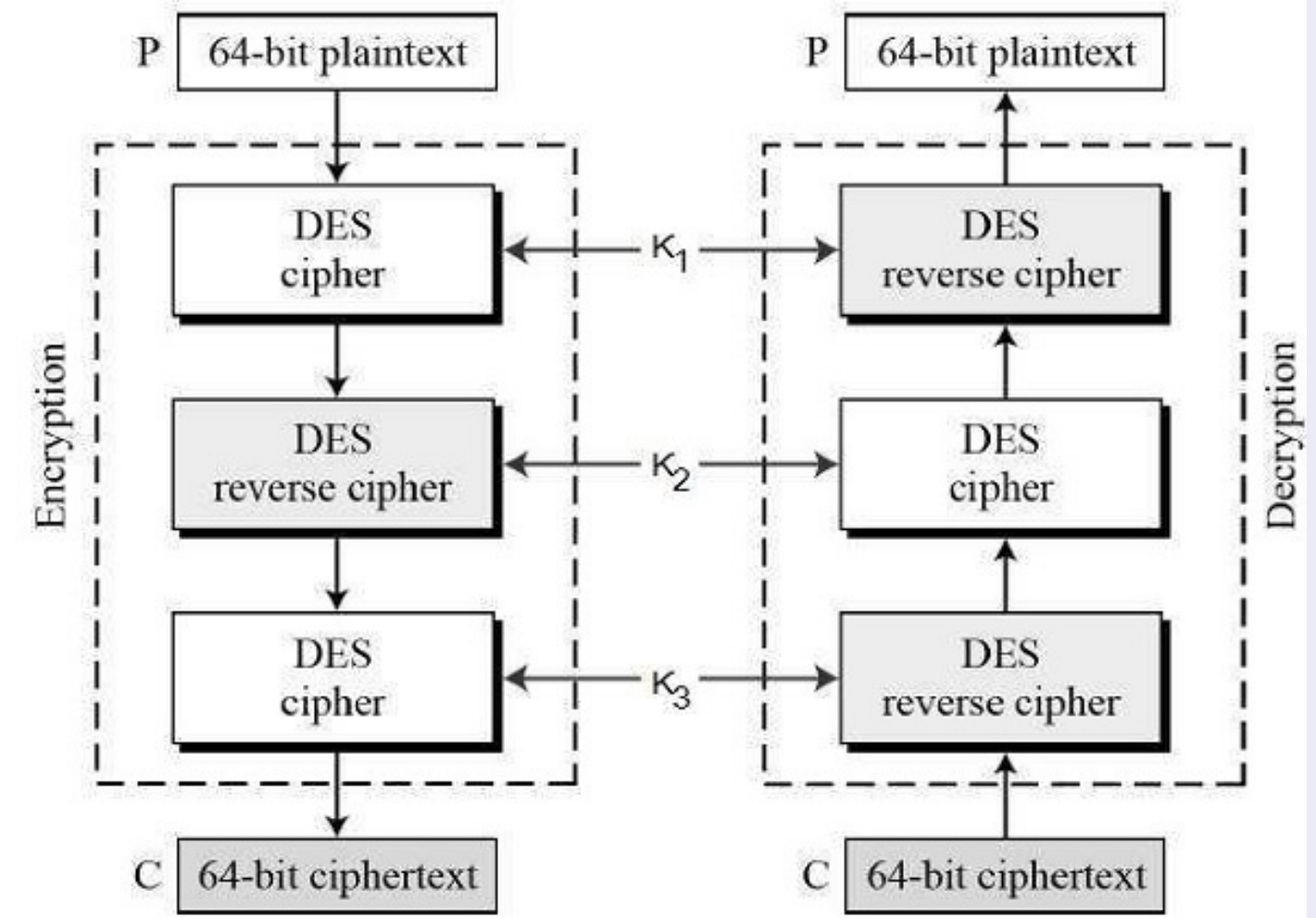


Triple DES with Two Keys (3DES with Two Keys)

- It uses two 56-bit keys K_1 and K_2, and 64-bit plaintext block.
- It produces 64-bit ciphertext block.
- It is also vulnerable to known-plaintext attack (meet-in-the-middle attack) to derive two keys K_1 and K_2.
- The expected running time of this attack is on the order of $2^{120-\log_2 n}$, where n is the number of plaintext-ciphertext pairs.



Triple DES with Three Keys (3DES with Three Keys)



K_1, K_2 and K_3: three 56-bit keys

DES (continued...)

Online Demo on DES Encryption and Decryption

- Generating parameters
- Symmetric key establishment
- Message encoding
- Encryption
- Decryption
- Message decoding

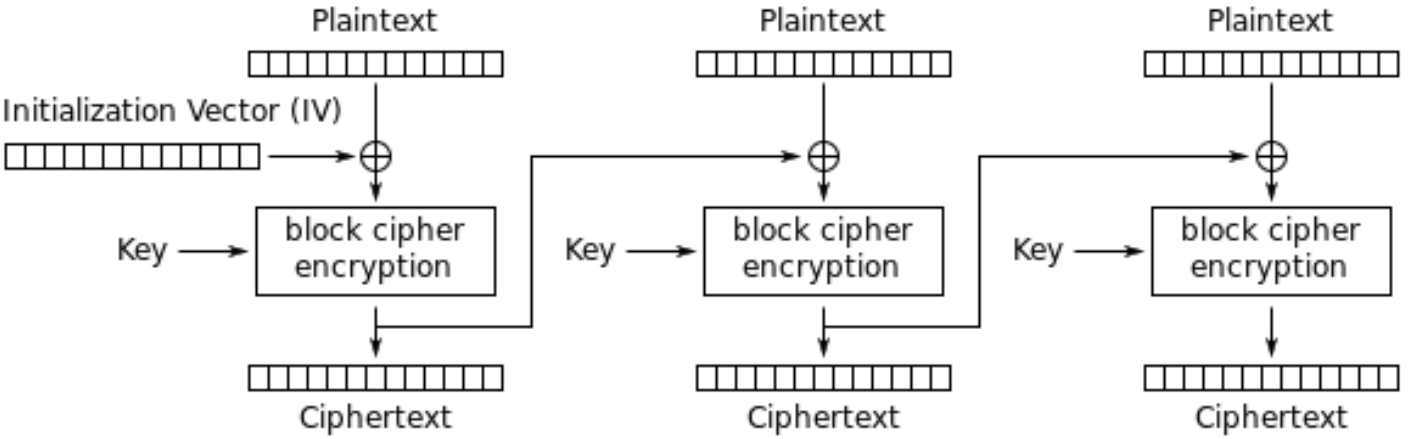
`https://cryptographyacademy.com/des/protocol/`

Symmetric-Key Encryption

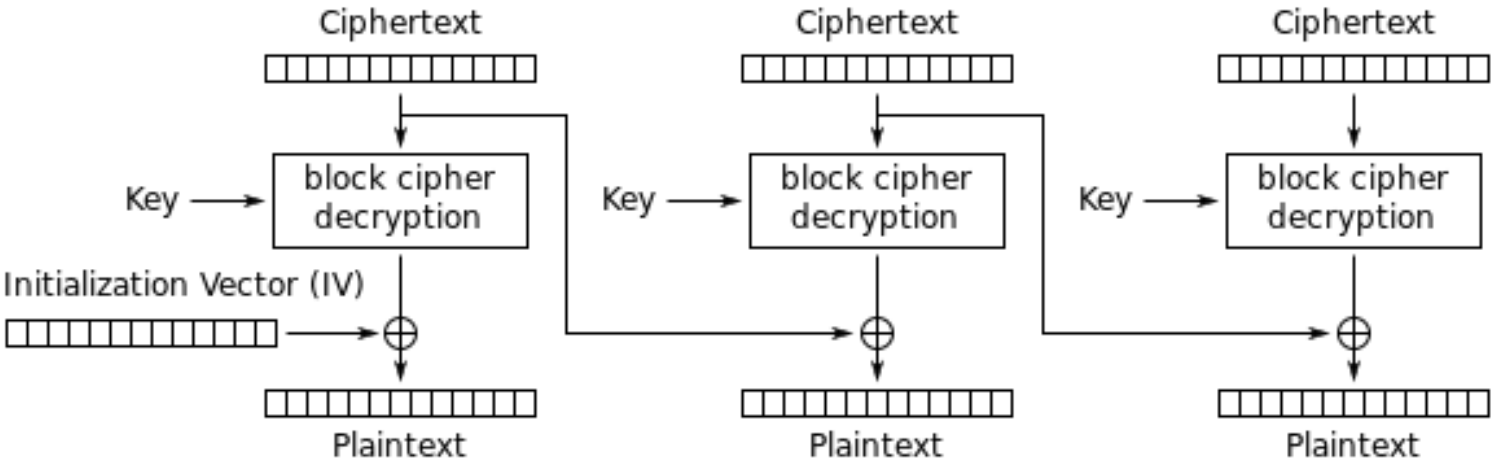
Various modes of operation of Data Encryption Standard (DES)

- Electronic Codebook Mode (ECB)
- Cipher Block Chaining Mode (CBC)
- Cipher Feedback Mode (CFB)
- Output Feedback Mode (OFB)
- Counter Mode (CTR)

Various modes of operation



Cipher Block Chaining (CBC) mode encryption



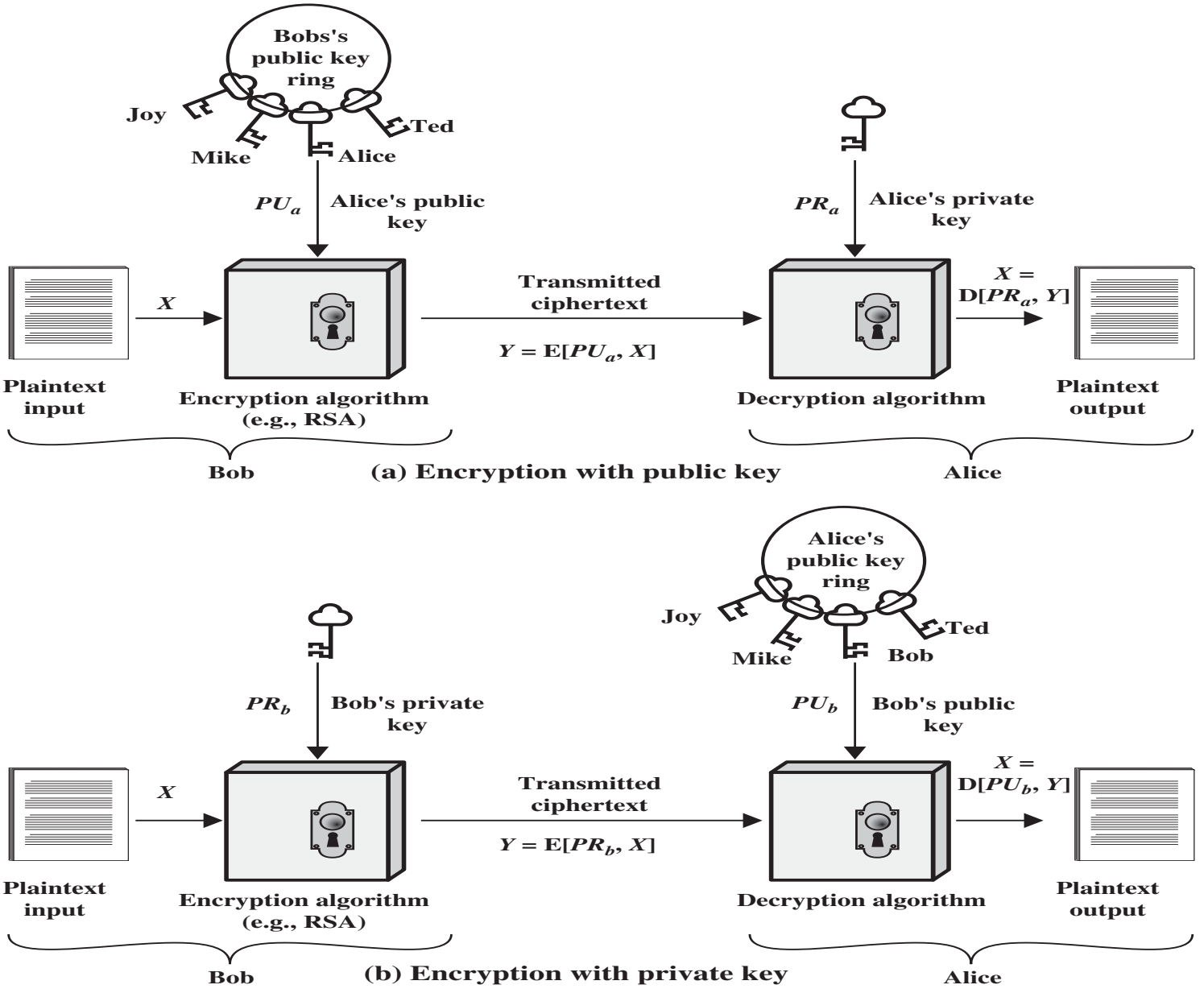
Cipher Block Chaining (CBC) mode decryption

Public-Key Encryption

Model of public key encryption

- Consider an encryption scheme consisting of
  - the set of encryption transformations $\{E_e : e \in K\}$
  - the set of corresponding decryption transformations $\{D_d : d \in K\}$, where K is the key space.
- The encryption scheme is said to be public-key or asymmetric-key, if for each associated encryption/decryption key pair (e, d), called public/private key pair, it is computationally "infeasible" to determine private key d from public key e.

Public-Key Cryptography



The RSA Algorithm

Introduction

- In 1978, Rivest, Shamir and Adleman at MIT, USA discovered a public-key cryptosystem, known as RSA algorithm.
- They received Turing Award (equivalent to Nobel Prize in Computer Science field).
- Their approach is based on elementary number theory concepts.
- The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and $n - 1$ for some n. A typical size for n is 1024 bits, or 309 decimal digits.

Inventors

Figure: Ronald L. Rivest

Inventors

Figure: Adi Shamir

Inventors

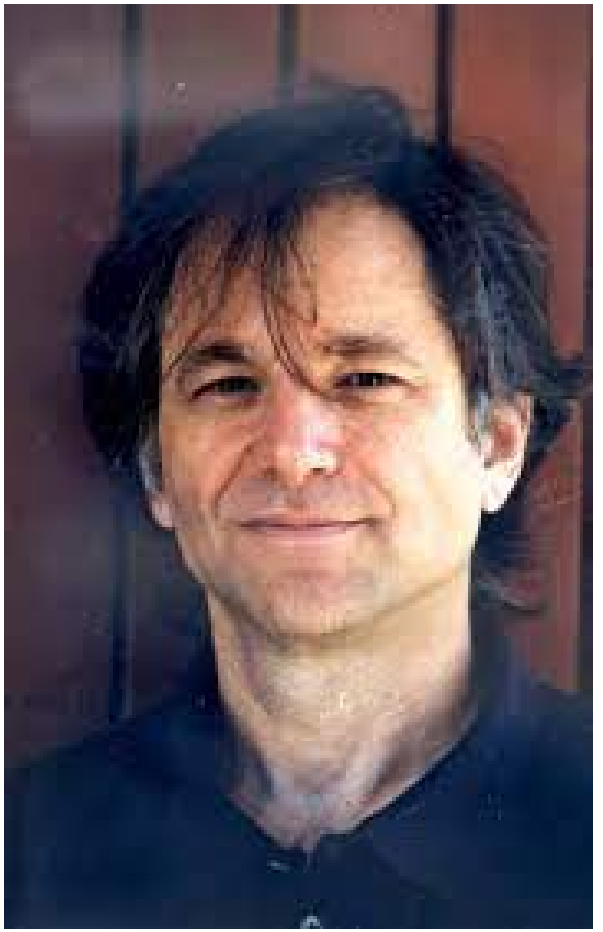


Figure: Leonard M. Adleman

Key Generation

Table: Key generation of the RSA algorithm

Select p, q	p and q both prime, $p \neq q$ (p and q are large)
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$ (Euler phi function)	
Select integer e	$\gcd(e, \phi(n)) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \mod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

The RSA Algorithm

Table: Encryption of the RSA algorithm

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

Table: Decryption of the RSA algorithm

Ciphertext:	C
Plaintext:	$M = C^d \pmod{n}$