A Practical Application of POSET: Hierarchical Access Control

Dr. Ashok Kumar Das

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

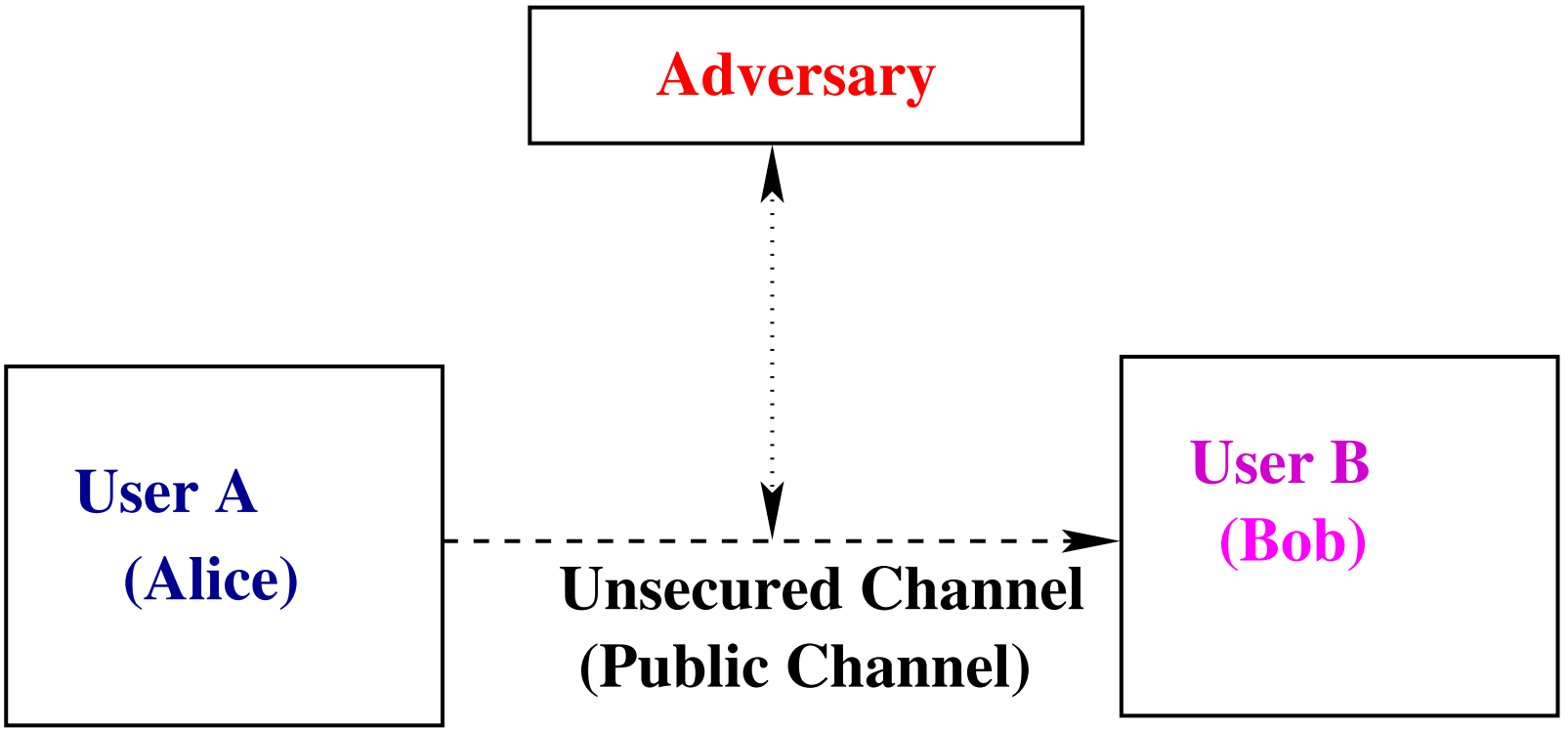
E-mail: *ashok.das@iiit.ac.in*
URL: `http://www.iiit.ac.in/people/faculty/ashokkdas`
`https://sites.google.com/site/iitkgpakdas/`

Overview of Cryptography

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.
- Cryptography is not the only means of providing information security, but rather one set of techniques.
- Now-a-days, cryptography has moved from an art to a science. Thus, cryptography is the science of keeping secrets secret.

Consider the following simple two-party communication model:



Introduction to Cryptography

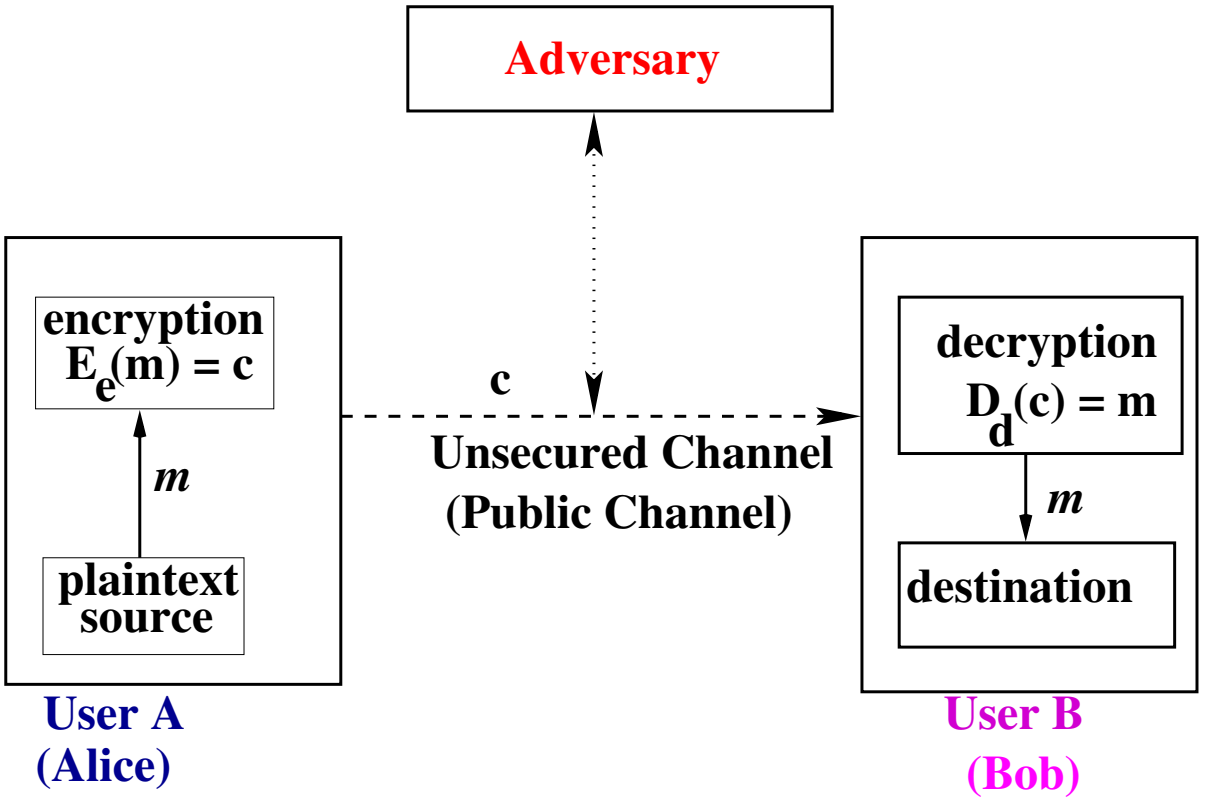
- An "**adversary**" is an entity in a two-party communication which is neither the sender nor the receiver, and which tries to defeat the information security service being provided between the sender and the receiver.
- A "**channel**" is a means of conveying information from one entity to another entity.
- An "**unsecured 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.

Introduction to Cryptography

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



$E_e(\cdot)/D_d(\cdot)$: encryption/decryption transformation using the encryption key e and decryption key d; $D_d = E_e^{-1}$; m: plaintext message and c: ciphertext message

Cryptology = Cryptography + Cryptanalysis

Introduction to Cryptography

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) where e is the encryption key and d is the corresponding decryption key, 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 10^6 decryptions per microsecond**
32	$2^{32} = 4.3 \times 10^9$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} years

Symmetric-Key Encryption

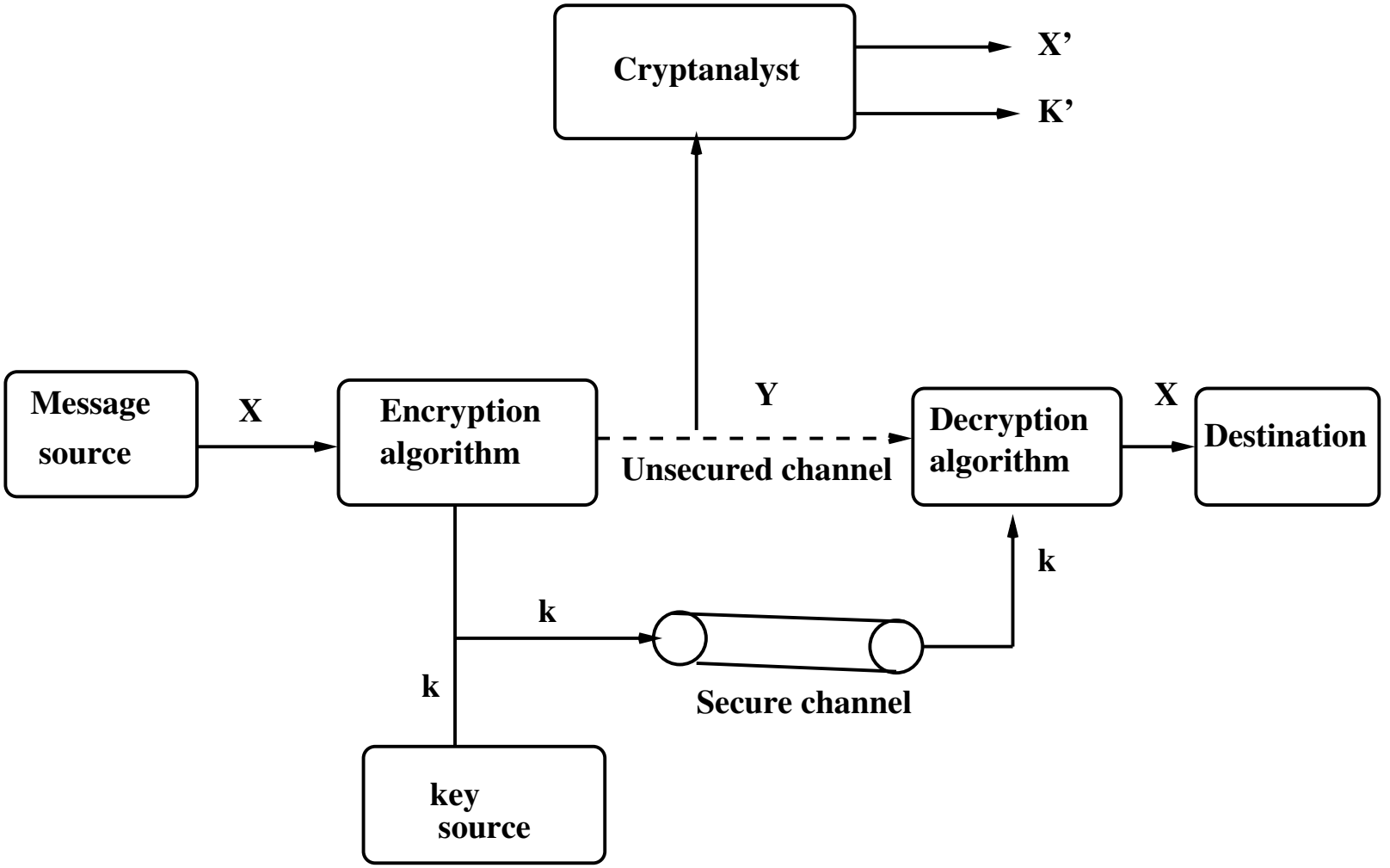


Figure: Model of conventional encryption

Public-Key Cryptography

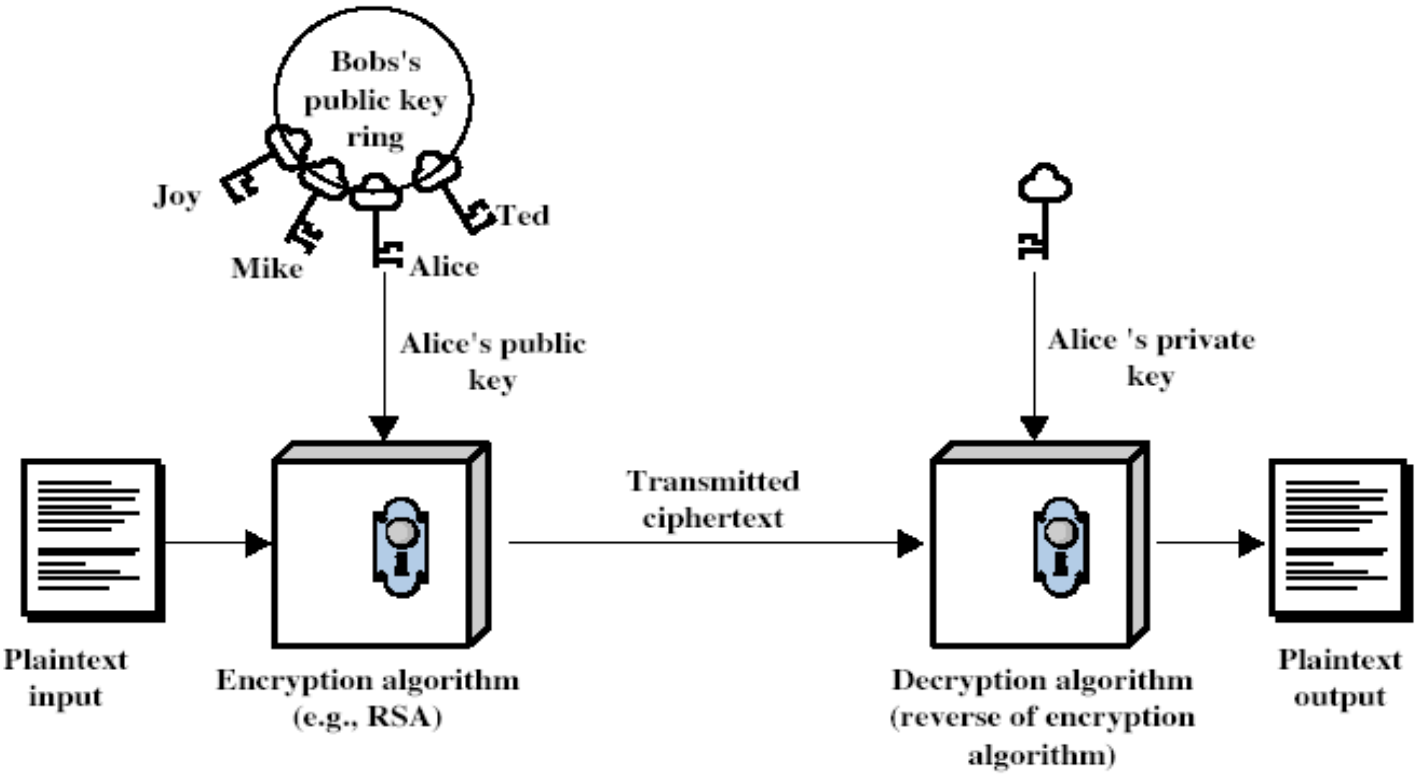


Figure: Model of public key encryption

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC)

- ECC makes use of the elliptic curves (not ellipses) in which the variables and coefficients are all restricted to elements of a finite field.
- Two family of elliptic curves are used in ECC:
  - prime curves defined over Z_p, that is, $GF(p)$, p being a prime.
  - binary curves constructed over $GF(2^n)$.