Cryptography Basics

Erukala Suresh Babu

Digitally signed by Erukala Suresh Babu
DN: cn=Erukala Suresh Babu, o=NITW, ou=CSE, email=esbabu@nitw.ac.in, c=IN
Date: 2019.08.27 06:44:12 +05'30'

Dr. E. Suresh Babu

Assistant Professor

Department of CSE

National Institute of Technology, Warangal

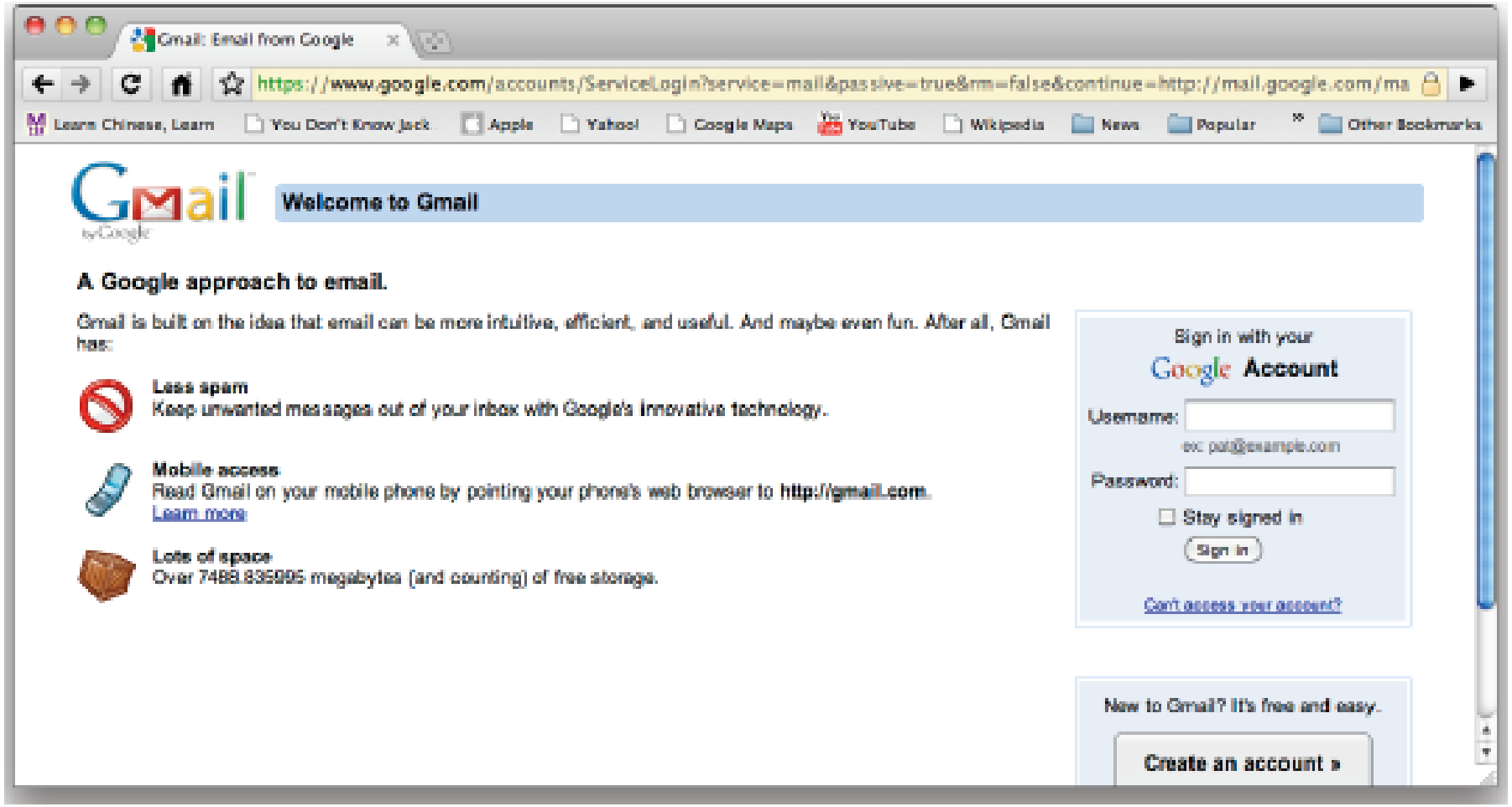
Outline

- Cryptography in Daily Life
- Introduction to Cryptography
  - ✓ Basic Terminology

Cryptography

- Did you use **any cryptography?**
  - ✓ **Today ?**
  - ✓ **Last week ?**

Cryptography



- **SSL** uses **Cryptography**

Everyday Cryptography

- ATM's
- On-Line Banking
- SSH
- Kerberos

What is Cryptography

What is Cryptography

- The Art and Science of keeping messages secure is **Cryptography**
- The word "Cryptography" is derived from Greek and when literally translated, means "**Secret Writing**."
- The whole point of cryptography is to keep the plaintext (or the key, or both) secret from **Eavesdroppers**

Eavesdroppers

- **Eavesdroppers** also called
  - ✓ **Adversaries**
  - ✓ **Attackers**
  - ✓ **Interceptors**
  - ✓ **Interlopers**
  - ✓ **Intruders**
  - ✓ **Opponents Or**
  - ✓ **Simply The Enemy**).

Basic Terminology

Basic Terminology

Plaintext

- An original message

Ciphertext

- The coded message

Enciphering/Encryption

- The process of converting from plaintext to ciphertext

Deciphering/Decryption

- Restoring the plaintext from the ciphertext

Cryptography

- The area of study of the many schemes used for encryption

Cryptographic System/Cipher

- A scheme

Cryptanalysis

- Techniques used for deciphering a message without any knowledge of the enciphering details

Cryptology

- The areas of cryptography and cryptanalysis

Definition of Cryptosystem

- A **General Cryptosystem** consists of a **5- tuple (*P, C, K, E , D*)**

where ***P, C, K*** are sets:

- ✓ ***P*** → **Plaintext space**
- ✓ ***C*** → **Cipher text space**
- ✓ ***K*** → **key space**
- ✓ $E = \{E_k\}_{k \in K}$,
- ✓ $D = \{D_k\}_{k \in K}$ are sets of functions

Functions of Cryptosystem

- Enciphering $E_k: P \rightarrow C$ and deciphering functions $D_k: C \rightarrow P$

  respectively which satisfy:

$$\forall k \in K \qquad D_k(E_k)(p) = p, \forall p \in P.$$

Kerckhoffs' Principle

- The Basic Assumption is
  - ✓ A cryptosystem should be secure even the system is completely KNOWN to the attacker
  - ✓ Only the key should be secure
- The Kerckhoffs' Principle states that the security of a cryptosystem should depend solely on the secrecy of the key.
  - ✓ **Crypto Algorithm are not Secret**

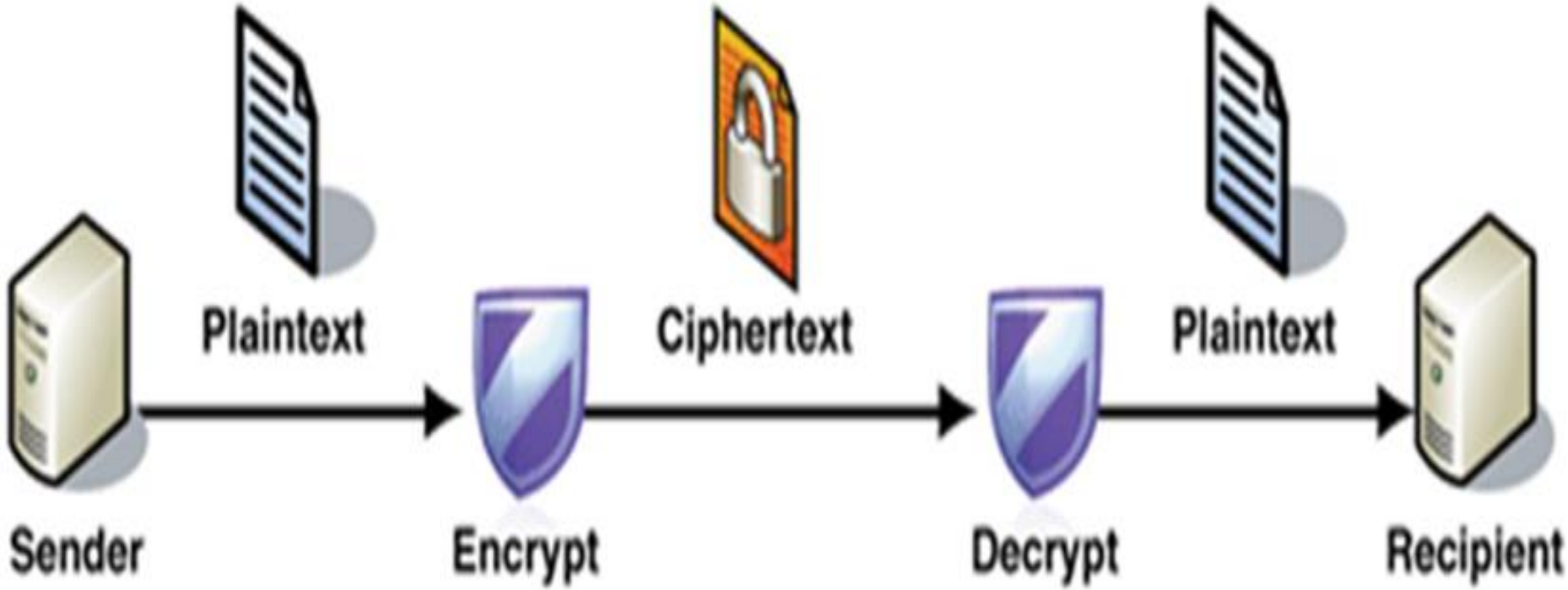
Kerckhoffs' Principle Assumption are useful

- Experience has shown that secret algorithm are weak when exposed to the Public
- Secret Algorithm never remain secret
- Better to Find Weaknesses for the Algorithm

Restricted Algorithm

- If the Secure Algorithm keeps the algorithm works in a secure manner, it is a **Restricted Algorithm.**
- Restricted Algorithms are woefully inadequate by today's standards

Restricted Algorithm



Advantages of Restricted Algorithm

- **Restricted Algorithms** are enormously popular for **Low-Security Applications.**

Limitations of Restricted Algorithm

- A Large Group Of Users cannot use them
  - ✓ Every time a user leaves the group everyone else must switch to a different algorithm.
  - ✓ If someone accidentally reveals the secret, everyone must change their algorithm.

Outline

- Cryptography in Daily Life
- Introduction to Cryptography
  - ✓ Basic Terminology

Thank U