CS641

Modern Cryptology

Lecture 1

Instructor

- Manindra Agrawal, Professor, Dept of CSE
- Contact: manindra@iitk.ac.in

Contents

Classical Ciphers: substitution and permutation ciphers, frequency analysis [2]

Modern Cryptanalysis: Known and chosen plaintext attacks, weakness of ciphers based on linear operations [1]

Private-key Encryption: DES, AES [7]

Public-key Encryption: RSA, ECC, Lattice-based [5]

Digitial Signatures: signatures based on RSA and ECC [1]

Hashing: MD5, SHA-3 [1]

Protocols: PKI, secret sharing, bitcoin and blockchain, etc. [3]

Reference Books

- Applied Cryptography, by Bruce Schneier.
- Introduction to Modern Cryptography, by Katz and Lindell

Grading

The course will have

- Midsem, weightage 25%
- Endsem, weightage 25%
- Assignments, weightage 50%
- 80+% marks $\Rightarrow$ A grade
- 20+% marks $\Rightarrow$ D or higher grade

Exams

- Exams will be take-home.
- Discussion is encouraged, but no copying.
- All students should form a group of size up to three. Each group needs to submit only one answer in examinations and assignments.

Copying Policy

- Any group caught copying in an assignment will get zero in that assignment.
- Any group caught copying in exams will get zero in that exam.

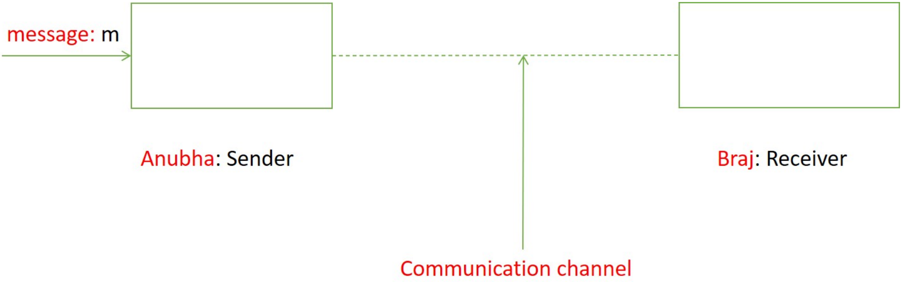
Schedule

- Discussion hour once a week. Date and time to be decided.
- Midsem during Feb 21-26, 2022
- Endsem during Apr 25-May 4, 2022

TAs

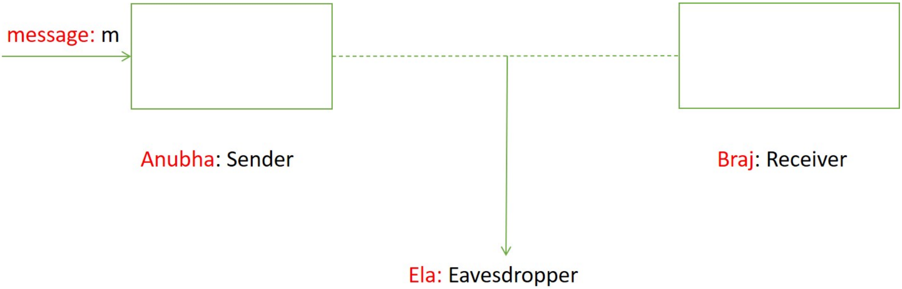
- Neelabjo Shubhashis Choudhury, neelabjo@cse.iitk.ac.in
- Mohammad Haseeb Qureshi, haseebq@cse.iitk.ac.in
- Harsika Diksha, mahesr@cse.iitk.ac.in
- P J Leo Evenss, leoevenss@cse.iitk.ac.in
- Prashant Shivhare, prashantsh@cse.iitk.ac.in
- Sharvari Ajay Oka, okasharvar@cse.iitk.ac.in
- Shashwat Vaibhav, shashwatv@cse.iitk.ac.in

Basic Structure



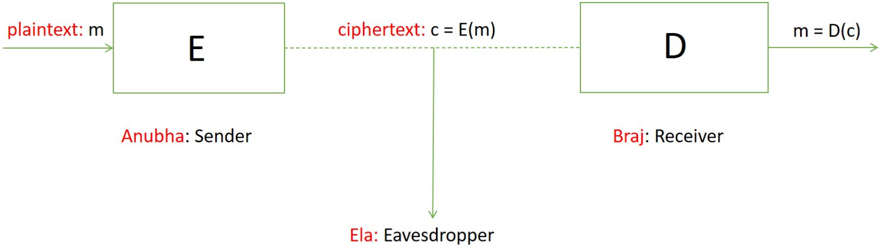
- What if the channel is insecure and message sensitive?

Basic Structure: Insecure Channel



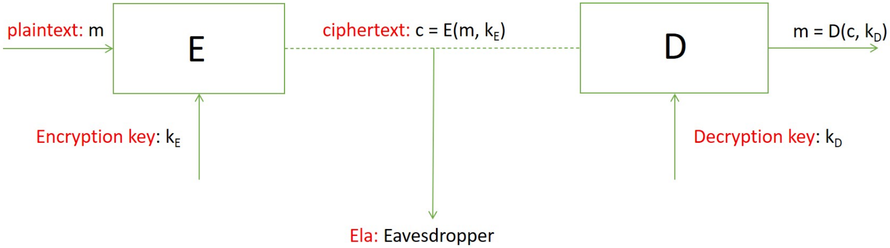
- How to stop Ela from reading message?

Basic Structure: Encoding-Decoding



- Operation E is called encryption and D is called decryption.
- What if Ela learns about D?

Basic Structure: Keys



- k_D and k_E must be kept secure.

Key Management

- If k_D and k_E never change, security is lost for ever in case of any leakage.
- Therefore, it is better to change keys at regular interval.
- Since k_E and k_D are "dual" of each other, both need to be changed simultaneously.
- How do Anubha and Braj get the new keys?
    - They can physically meet once a while.
    - They can agree on a large set of keys at the start and change the usage by simply sending the key number.
- We will discuss secure methods of key exchange later.

Key Size

- Let $s = |k_D|$.
- If s is small, Ela can run through all the 2^s possible values of k_D, decrypt the ciphertext, and choose the value that results in sensible plaintext.
- Therefore, to ensure security, s must be chosen large.

Key Size

- How large?
  - Fastest supercomputer at present (Fugaku) runs at ≈ 415 petaflops.
  - Assuming that one value of k_D can be checked in one operation (very generous assumption), this computer can check $< 10^{18}$ values in a second.
  - This translates to $< 10^{23}$ values in a day, $< 10^{26}$ values in a year, and $< 10^{36}$ values in 10 billion years (life of the universe).
  - As $10^{36} < 2^{120}$, $s = 128$ suffices.

Caeser Cipher

For every letter ℓ of message m, replace ℓ by third letter from ℓ in the alphabet.

- Example: $m =$ Cryptography becomes $c = E(m) =$ Fubswrjudskb.
- One of the earliest known use of encryption (around 50 bce).
- Very simple to apply.
- Very easy to decipher once the algorithm is known.
- Even making shift amount as key does not help since the possible values are very small ($= 26$).

Substitution Cipher

$k_E : [a - z] \mapsto [a - z]$, k_E a permutation.

$E(\ell_1 \ell_2 \cdots \ell_n) = k_E(\ell_1) k_E(\ell_2) \cdots k_E(\ell_n)$.

$k_D = k_E^{-1}$, and $D = E$.

- Number of possible keys equals $26! \approx 10^{26}$, a sufficiently large number.
- A generalization of Caeser Cipher.
- Used for a long time.
- Can be broken by frequency analysis.