Week 3

Lecture 1

Modern Symmetric key Ciphers

Lecture 2

Properties of Numbers III,

Workshop 3: Workshop based on Lectures in Week2

Quiz 3

Mode Ciphers

COMP9

Lecture 1

Modern Symmetric key Cryptography

Lecture 1

1.1 Modern Symmetric Ciphers
- Model and Design Principles
- Stream Ciphers and Block Ciphers

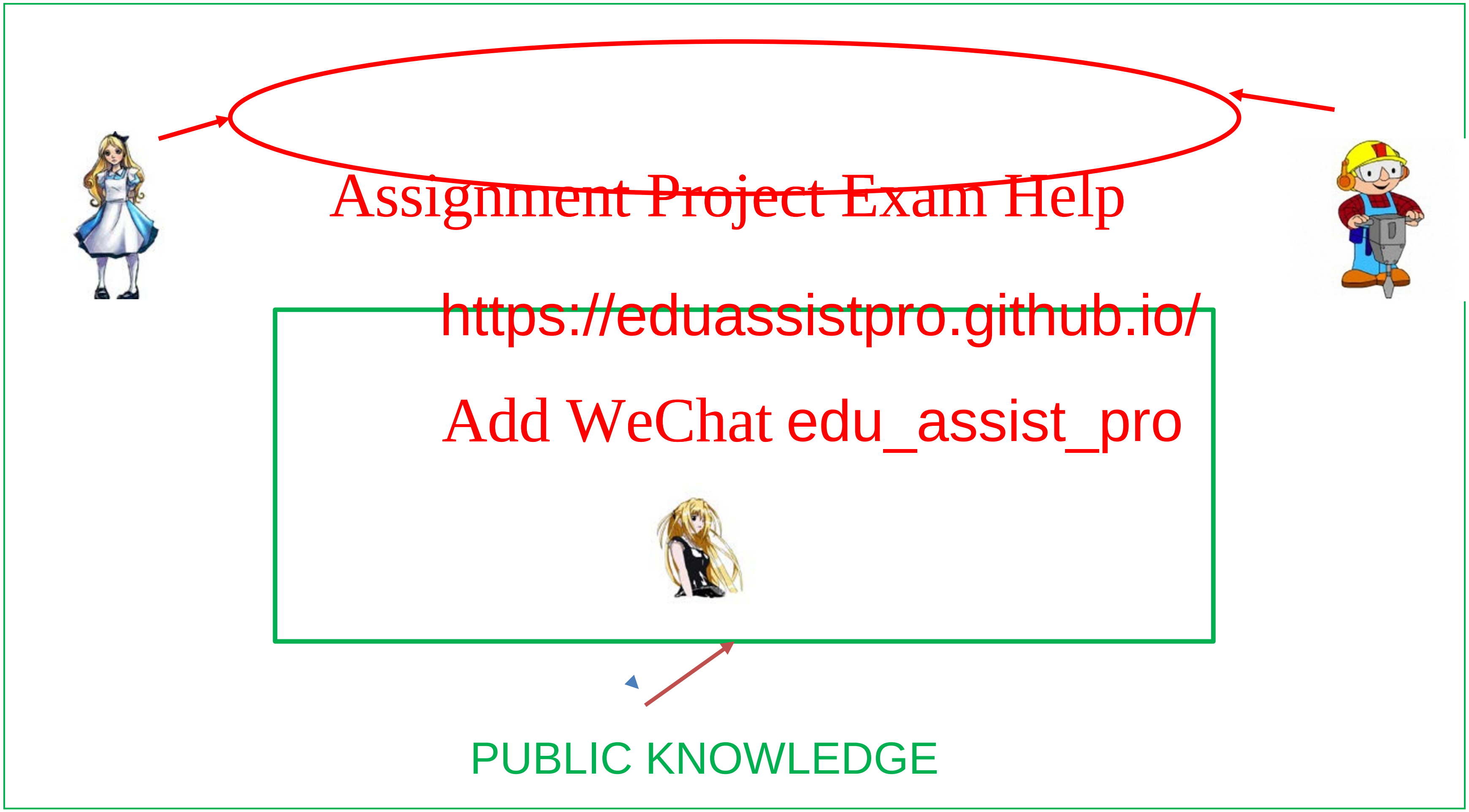
1.2 One-Time Pad Encryption
- Vernam Cipher
- One-Time Pad
- Perfect Secrecy

1.3 Fiestel Cipher
- Motivation and General ideas
- Cipher Terms and Structure
- Data Encryption Standard
- A worksheet

1.4 Modes of Block Ciphers
- Codebook Mode
- Cipher Block Chain
- Stream Cipher modes

Recap: Symmetric Key Cyptosystems

Modified From:Stallings Figure 2.1:



Recap (Week 2)

- 1.1 Symmetric Cipher Models
  - Basic Terminology
  - Model and Logical View
  - Basic Requirements and Kerckhoffs'sprinciple
- 1.2 Security
  - Characterization of S
  - Attacks on Symmet
- 1.3 Classical Ciphers
  - Substitution CiphersCaesar and Affine Ciphers
  - Monoalphabetic Substitution Ciphers
  - Transposition CiphersRail fence cipher
  - Row Transposition Cipher
- 1.4 Cryptanalysis of Classical Ciphers
  - Caesar Cipher
  - Affine Cipher
  - Monoalphabetic Substitution Ciphers
- 1.5 Complex Ciphers
  - Polyalphabetic Ciphers, VigenèreCipher

Numbers, gcd, primes,
Extended GCD algorithm
erse mod n
er Phi function

1.1 iphers

COMP9

Lecture 1

Design Principles

- These are two major kinds of ciphers, which differ in the way the plaintexts are encrypted.

- **Block Cipher**: A block cipher takes a fixed length plain text message block (for example, 64 or ces a cipher text block of the same length as t
  – DES (56), Tripl wfish() and AES (128)

- **Stream Cipher**: Takes a key of fixed tes a key stream in a pseudo random fashion with large period; this key stream is then combined with the plain text message stream on a bit by bit basis to form a cipher text stream.

  – RC4, A5, BlueTooth cipher etc.

Stream and Block Ciphers

- Unit of stream operation can be “bit by bit” or “byte by byte” or “symbol by smbol”, it encrypts one unit of plain text stream at a time. Useful for processing stream-based data voice, connection-traffic etc.

eration is always of a block of information, generally n-bit blocks. Useful in many situations of data traffic.

.

From:Stallings Figure 4.1:

1.2 yption

COMP9

Lecture 1

Vernam Cipher

- We looked at Vegenere Cipher, a simple polyalphabetic substitution cipher.
- ith plaintext symbol is handled by Caesar cipher with key: $k_{(i \bmod d)}$

- The idea is very simple, a key is a multiple letter word: $K = k_1\ k_2 \dots k_d$
- $P = p_1\ p_2 \dots p_d\ p_{d+1}$

- $C = c_1\ c_2 \dots c_d\ c_{d+1}\ c_{d+2} \quad {}_{2d}\dots.$
- Encryption: $E(K,P) = C$, where $c_i = p_i$

- Decrypton: $D(K,C) = P$, where $p_i = c_i - k_i \bmod 26$
- Here we extend the size of the key to be equal to the message ($d = n$). The resulting cipher is Vernam.
- The scheme can be defined over any alphabet (mod m).
- It is also called as One-Time-Pad.

One-Time Pad Definition

- Defined over binary messages.
- Let ⊕ denote exclusive or symbol. Let [0,1] be binary alphabet.
  - $0 \oplus 0 = 1 \oplus 1 = 0$;
  - $0 \oplus 1 = 1 \oplus 0 = 1$.

- We will extend the o any sequence over [0.1].
- If A, B, C are vector

$A \oplus B = C$; then $B = A \oplus C$; $A \oplus A = 0$; = 0

- Suppose Alice wishes to send a message to Bob and they have previously established a shared secret ke .
  The cipher text is formed by exclusive-oring the message with the key:

  $$C = M \oplus K = 1101100.$$

  Decryption is trivial: the message could be obtained by the same process, i.e. by addition of K to C.

  $$M = C \oplus K = 0110111.$$

One-Time Pad Properties

- An extension of Vernam Cipher for binary messages.
- Here the key is as long as the message.
- For each message you need a distinct random key.
- Encryption and [illegible] xactly same, XOR with the key.

THE UNIVERSITY OF MELBOURNE

Perfect Secrecy

- What does it mean for an encryption scheme to be perfectly secure?

- Let us look at the approach taken by Shannon to answer this question.

- An encryption sche **tional security** if the cipher text generate eal sufficient information to brea to an unlimited amount of computational power.

- In other words, the adversary cannot n nowledge to reverse the encryption by watching any amount of cipher text without access to the key. Shannon in his seminal paper* in 1949 showed that one-time pad encryption is perfectly secure.

* C.E. Shannon. Communication in presence of noise. IEEE, 37:1021, 1949.

Probability Basics

- Let S be a sample of space of events.
- $S = \{x_1, x_2, x_3, \ldots, x_n\}$
- An event A is a subset of S, probability of A satisfies:
- $0 \leq P(A) \leq 1$.
- $P(S) = 1$, $P(\emptyset) = 0$.
- If $E \subset F$, $E, F \in S$, t
- $P(E) + P(E^c) = 1$, where $E^c = S \setminus E$.

- Conditional Probability: If $A, B \in S$ are any events in S and $P(B) = 0$, then the conditional probability relative to the event B is given by
- $P(A \mid B) = P(A \cap B) / P(B)$

Perfect Secrecy

- Let x: input, y: output
- Perfect Security implies: $P_{X|Y}(x|y) = P_X(x)$
- The one-time pad offers perfect secrecy. Let us make it more precise what this means.

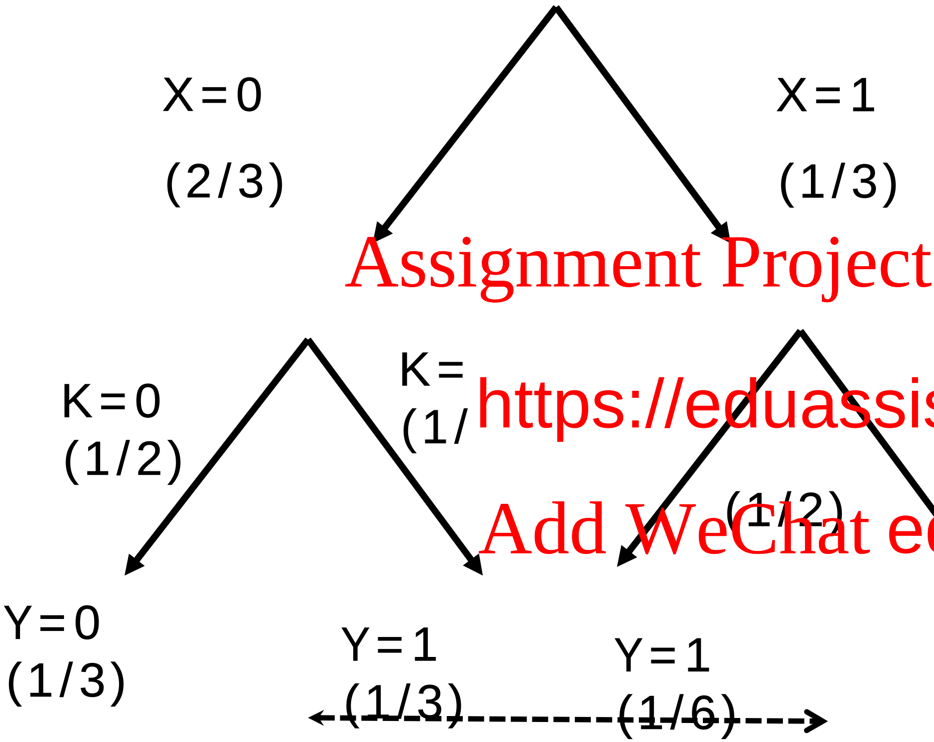
- Let us assume that t r 1) and key space is also binary. Assume that A chooses m ter of the time, i.e Probability that the message is 0 is eq =0) = 1/4. Perfect secrecy means knowing this fac y (E) should not get more information by observing the cipher message ($C = M \oplus K$). i.e. The condition probability, $P(M = 0 \mid C = 1)$ should not be different from apriori probability $P(M=0)$.

- This means that seeing the cipher text C does not increase the adversary's knowledge about the message

Another example

- Let message space be 0 or 1, i.e X = 0 or 1.
- Assume that the Adversary a priori knows that probability that (X = 0) is 2/3.
- i.e, P(X=0) = 2/3, th
- Suppose Y =1 was observed at the out er.
- We want to prove P(X=0|Y=1) = P(X=0).
- **This equivalent to : Seeing the cipher text does not increase the adversaries knowledge about the underlying message.**

Graph of one bit encryption



Computation of probabilities: message is 0 or 1

ey is chosen
andomly

P(Y=1)= 1/3+1/6=1/2

$$P(X=0|Y=1) = P(X=0 \ \Lambda \ Y=1) / P(Y=1) = ((2/3)(1/2)) / (1/2) = 2/3 = P(X=0)$$

General Result

- When X and Y are long sequences of 1's and 0's of length n.

- Theorem: $P(X{=}m|Y{=}c) = P(X{=}m)$.

- Proof depends critically on the fact th ed according to uniform distribution,

- i.e, $P(K{=}k_1) = 1/2^n$,

Implications

- In practice, messages may be biased; could be observed by the adversaries.

- Requirement: Encryption transformation should distribute messages to cipher space fairly uniformly irrespective of known apriory statistics of the messages.

- One-time pad analy andom secret key pad at least the size as the message, we can ac ect secrecy.

- Basically, the random key, which is as ssage, hides the message completely leading to the perfect "confusion" to the adversary by perfectly "diffusing" the statistical structure of the plain text to the entire ciphertext.

- However, one-time pad is not practical.

THE UNIVERSITY OF MELBOURNE

Two-time pad is Dangerous

- One-time pad is not practical. It demands a key as long as the message.
- What happens if we reuse the one-time pad used in the encryption?

- $C_1 = M_1 \oplus K$; $C_2 = M_2 \oplus K$; then

- $C_1 \oplus C_2 = M_1 \oplus M_2 \oplus \quad \oplus \quad \oplus$

- Even though $M_1 \oplus M$ … aks information about both M_1 and M_2. Also, in … messages M_1 or M_2 is available to the adversary, then he/she can

- This attack implies that you need a new ke … age.

- The idea is used in attacking Vegenere cipher (same key-pad is added many times).

- This type of analysis helped Allied in World Wars in 20th Century. Germans made this mistake in the war times!. Turing led Allied team made use of such vulnerability during initial key broadcast by Germans, which eventually helped to crack the master key used for the day.

Stream Ciphers

- How to we define a practically useful One-Time pads?

- An idea is to generate a long stream based on a short key and use it as a keystrea pad scheme. The re is “stream Cipher”.

- Stream cipher in general takes a key and a random nonce (Initial Vector(IV))as input and outputs a keystream of arbitrary size. The keystream is then xored with the plaintext to obtain a ciphertext.

Modified From:Stallings Figure 4.1a:

Modern Stream Ciphers

- Stream ciphers are extensively employed in modern communication networks.

- They are of the algorithm of choice in Light Weight Cryptographic applications.

- eSTREAM: ECRY European stream cipher project in the last decade gave impetu pment of the subject.

- They are every where: BlueTooth, Phones, browsers etc.

- We will revisit this idea when we study Block Ciphers in Stream Cipher mode.

1. hers

COMP9

Lecture 1

Block Ciphers

- Encrypts blocks of n characters/bits of plain text simultaneously outputting blocks of cipher texts.
- Same key is used for many different message blocks.

- Fundamental buildi hical functions.

- Examples include h tors, message authentication codes etc.

- **Confusion and diffusion principles:**
- **Diffusion** dissipates statistical structure of plaintext over bulk of ciphertext.
- **Confusion** makes relationship between ciphertext and key as complex as possible.
- Generally diffusion is created by permutations and confusion is created by substitution.

Product Ciphers and Fiestel Ciphers

- A **product cipher** combines two or more transformations so that resulting cipher is more secure than the individual components by making use of confusion and diffusion principles.

- A **substitution-permutation cipher** is a product cipher made up of number of stages e ermutation. The operations of substi onsible for effecting the confusion and diffu

- An **iterated block cipher** is a block ci sequential repetition of an iterated function called a round f
- The parameters of iterated block ciphers are r: number of rounds; n: block length; k: bit-size of key, K from which r subkeys (round keys) k_i's are derived.

- **Fiestel Cipher** is an example of an iterated block cipher.

Fiestel Block Cipher

- **Fiestel** ciphers are iterative ciphers; they repeat a given operation several times in rounds.
- Each round will have the following distinct operations:

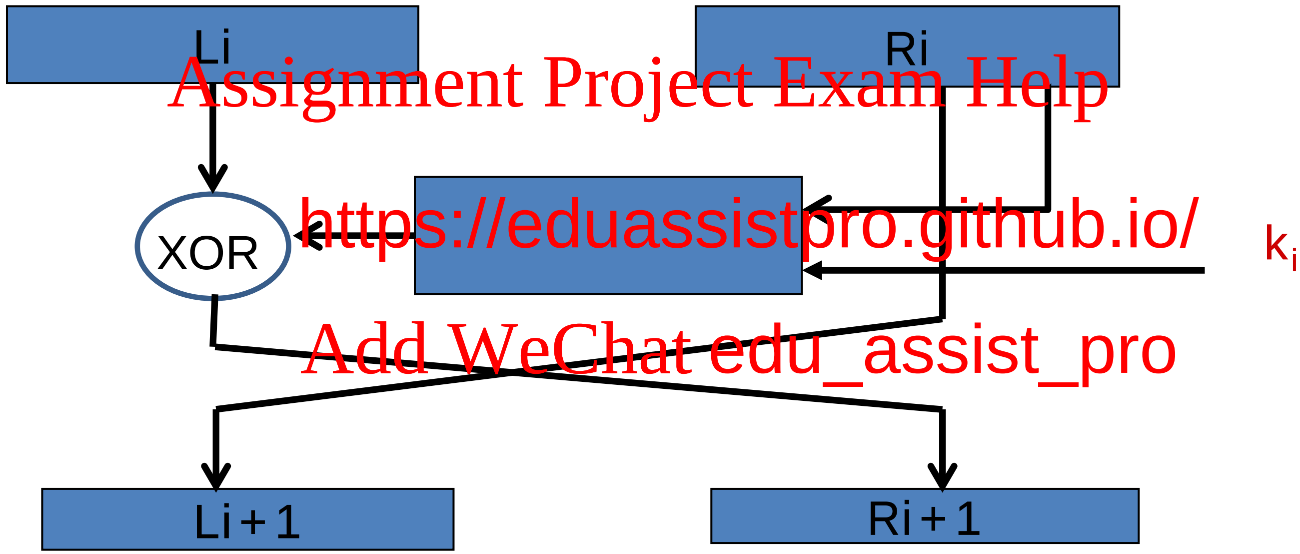
- **Substitution**: Each a block are replaced with a correspondin s.

- **Permutation**: A certain perimutation i ch transformed ciphertext bits.

- The above round operations are repeated certain number of rounds.

Fiestel Block Cipher, cont.

For such a cipher, the input key is used to produce round keys $k_1, k_2, \ldots, k_r$. The message is initially divided into two parts, namely left and right halves, L and R.
For each of r rounds, the following operations are executed.



After r rounds, the final left and right haves are swapped and concatenated to form the cipher text.
The design of a good function f is partly ``ART'' and partly ``SCIENCE''.

Data Encryption Standard (DES)

- IBM's 1974 submission for a standard.
  A Fiestel cipher
  Block size: n = 64,
  keysize = k = 56 bits.

  The key is specifie of parity.
  Number of rounds

  Strengthening DES:
  DESX: Apart from 56 bit key K, choo bit keys
  K_I and K_O, then we encrypt

  C = K_O ⊕ DES(K, M ⊕ K_I)

  This method increases effective key length to 199-t, where t is a quantity related to adversaries' cryptanalytic assumptions where the adversary is able to collect 2^t matching input-output pairs.
- Read the textbook for more details on DES.

Feistel Cipher Structure

From:William Stallings 5th Edition:

Feistel Cipher Decryption

From:William Stallings 5th Edition:

Strengths, properties and attacks on DES

- Each bit of cipher text depends on all bits of the key and all bits of the plain text.

- No statistical relat ipher visible.

- Altering a key bit or a plain text bit each cipher bit with probability close to half.

- Altering a cipher bit should result in unpredictable change in plain text block.

Cryptanalysis of DES

- Empirically it is found that DES is safe.

- Exhaustive search -- Brute force. 2^{56} computations.

  Differential cryptanalysis

- Chosen plain text a

- Not realistic -complexity 2^{47} computati

  Linear cryptanalysis
- Complexity : 2^{43} computations.
- The main drawback is limited key space.

- The new standard for encryption now is AES which has key space >= 2^{128}.

Advanced Encryption Standard (AES)

- DES is not recommended as it has small key space and have known theoretical attacks.

- Financial Systems still use a modification of DES such as Triple-DES, which also has sign ve small block size)

- So, NIST worked with crypto commu to develop an Advanced Encryption Standard (AES)

- In October 2000, NIST accepted Rijndael as the AES in Oct-2000.

- It is proposed by cryptographic researchers: Dr. Joan Daemen and Dr.Vincent Rijmen.

AES Algorithm

- Stallings discusses AES algorithm in detail.
- It is not a Fiestel cipher, but still iterative.
- Main design requir
  - Should withstand all known attack
  - It should have flexible implementation, to be able to run on varieties of platforms and CPUs.
  - It should have a simple design features.

How do you make Encryption more complex?

- One can increase block size n and also look for different functions for encryption.

- In practice, data comes in many forms. W ecan modify the function for different modes.

- These practical modes are developed ing on using encryption. More on Chapter 7 of the t

1.4 phers

COMP9

Lecture 1

Modes of Operations

- NIST defined five basic modes of usage of block cipher.
- They are generic: can be use with any block cipher.

- Five modes:

  - Electronic Cod
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
  - Counter (CTR)

rypt and Decrypt
ns

Uses only Encrypt functions

Used like a stream cipher

Mode of Operations

From:Stallings Table 7.1:

You will learn more from the textbook.

Week 3

Lecture 1

Modern Symmetric key Ciphers

Lecture 2

Finite Field mathematics,

Workshop 3: Workshop based on Lectures in Week2

Quiz 3