JAYOTI VIDYAPEETH WOMEN'S UNIVERSITY, JAIPUR
Government of Rajasthan established
Through ACT No. 17 of 2008 as per UGC ACT 1956
NAAC Accredited University

Faculty of Education and methodology

Department of Science and Technology

Faculty Name- Jv'n Narendra Kumar Chahar (Assistant Professor)

Program- B.Tech 8thSemester

Course Name– Cryptography and Network Security

Session no.: 19

Session Name- Modern Private key ciphers

Academic Day starts with –

- Greeting with saying **'Namaste'** by joining Hands together following by 2-3 Minutes Happy session, Celebrating birthday of any student of respective class and **National Anthem**.

Lecture starts with- quotations' answer writing

Review of previous Session **– Stream Ciphers and the Vernam cipher**

Topic to be discussed today- Today We will discuss about **Modern Private key ciphers**

Lesson deliverance (ICT, Diagrams & Live Example)-

- Diagrams

Introduction & Brief Discussion about the Topic**– Private Key Ciphers**

Modern Private Key Ciphers

Modern Private Key Ciphers (part 1)

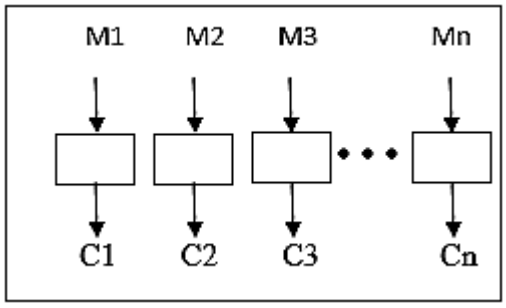
Now, concentrate on the modern encryption systems and these usually consider the message as a sequence of bits e.g. As a series of ASCII characters concatenated.

This has two broad families of methods: stream ciphers and block ciphers

Block Ciphers

In a block cipher, the message is broken into blocks, each of which is then encrypted (i.e., like a substitution on very big characters - 64-bits or more)

The most modern ciphers we will study are of this form:



Shannon's Theory of Secrecy Systems

Claude Shannon wrote some of the pivotal papers on modern cryptology theory in 1949 and developed the concepts of entropy of a message, redundancy in a language, and theories about how much information is needed to break a cipher. He also defined the concepts of computationally secure vs unconditionally secure ciphers.

He showed that the Vernam cipher is the only currently known unconditionally secure cipher, provided the key is truly random and also showed that if try to encrypt English text by adding to other English text (i.e., a Book cipher), this is not secure since English is 80% redundant, giving ciphertext with 60% redundancy, enough to break

A similar technique can also be used if the same random key stream is used twice on different messages, the redundancy in the messages is sufficient to break this. As discussed earlier, exhaustive key search is the most fundamental attack, and is directly proportional to the size of the key. It can tabulate these for reasonable assumptions about the number of operations possible (& parallel tests):

Key Size (bits)	Time (1us/test)	Time (1us/106test)
24	8.4 sec	8.4 usec
32	35.8 mins	2.15 msec
40	6.4 days	550 msec
48	4.46 yrs	2.35 mins
56	~2000 yrs	10.0 hrs
64	~500000 yrs	107 days

As the ultimate limit, it can be shown from energy consumption considerations that the maximum number of possible elementary operations in 1000 years is about: 3 x 10 ^(48)

Similarly, can show that if need say 10 atoms to store a bit of information, then the greatest possible number of bits storable in a volume of say the moon is: 10 ^(45)

If a cipher requires more operations, or needs more storage than this, it is pretty reasonable to say it is computationally secure e.g. to test all possible 128-bit keys in Lucifer takes about 3 x 10 ^(48) encryptions, needing 10 ^(19) years

Reference-

1. **Book:** William Stallings, "Cryptography & Network Security", Pearson Education, 4th Edition 2006.

QUESTIONS: -

Q1. Give an overview about Shannon's Theory of Secrecy Systems.

Next, we will discuss more about Substitution-Permutation Ciphers.

- Academic Day ends with-
  National song 'Vande Mataram'