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.: 20

Session Name- Substitution-Permutation 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 **– Modern Private key ciphers**

Topic to be discussed today- Today We will discuss about **Substitution-Permutation Ciphers**

Lesson deliverance (ICT, Diagrams & Live Example)-

- Diagrams

Introduction & Brief Discussion about the Topic**– Substitution-Permutation Ciphers**

Substitution-Permutation Ciphers

In his 1949 paper Shannon also introduced the idea of substitution-permutation (S-P) networks, which now form the basis of modern block ciphers. An S-P network is the modern form of a substitution-transposition product cipher. S-P networks are based on the two primitive cryptographic operations we have seen before

Substitution Operation

A binary word is replaced by some other binary word and the whole substitution function forms the key

if use n bit words, the key is 2^(n)! bits, grows rapidly.

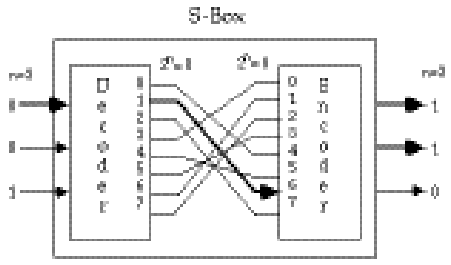

Fig 2.1 Substitution Operation

It can also think of this as a large lookup table, with n address lines (hence 2^(n) addresses), each n bits wide being the output value and these will call them S-boxes.

Permutation Operation:

Here, a binary word has its bits reordered (permuted) and the re-ordering forms the key. If use n bit words, the key is n! bits, which grows more slowly, and hence is less secure than substitution.

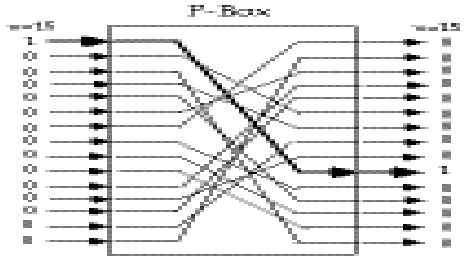

Fig 2.2 - Permutation or Transposition Function

This is equivalent to a wire-crossing in practice (though is much harder to do in software) and it will call these P-boxes

Substitution-Permutation Network.

Shannon combined these two primitives and called these *mixing transformations.*

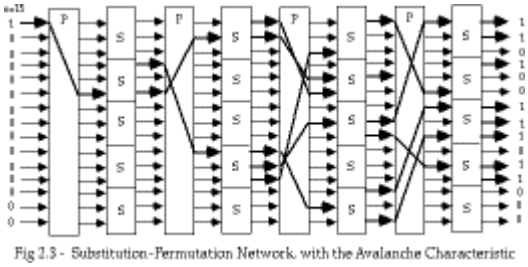

Fig 2.3 - Substitution-Permutation Network, with the Avalanche Characteristic

Shannon's mixing transformations are a special form of product ciphers were

S-Boxes provide confusion of input bits and P-Boxes provide diffusion across S-box inputs.

In general, these provide the following results:

Avalanche effect

Where changing one input bit results in changes of approx half the output bits

More formally, a function f has a good avalanche effect if for each bit i,0<=i<m, if the 2^(m) plaintext vectors are divided into 2^(m-1) pairs X and X_(i) with each pair differing only in bit i; and if the 2^(m-1) exclusive-or sums, termed avalanche vectors

V_(i) = f(X) (+) f(X_(i))

Are compared, then about half of these sums should be found to be 1.

Completeness effect

where each output bit is a complex function of all the input bits

More formally, a function f has a good completeness effect if for each bit j,0<=j<m, in the ciphertext output vector, there is at least one pair of plaintext vectors X and X_(i) which differ only in bit i, and for which f(X) and f(X_(i)) differ in bit j

Practical Substitution-Permutation Networks

In practice, we need to be able to decrypt messages, as well as to encrypt them, hence either:

- have to define inverses for each of our S & P-boxes, but this doubles the code/hardware needed, or
- define a structure that is easy to reverse, so can use basically the same code or hardware for both encryption and decryption

Horst Feistel, working at IBM Thomas J Watson Research Labs devised just such a structure in early 70's, which we now call a Feistel cipher

- the idea is to partition the input block into two halves, L(i-1) and R(i-1), and use only R(i-1) in each round i (part) of the cipher
- the function g incorporates one stage of the S-P network, controlled by part of the key K(i)known as the ith subkey

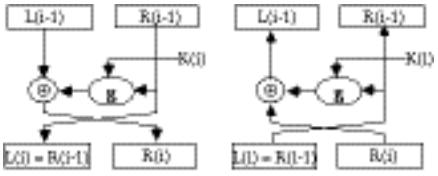

Fig 2.4 - A Round of a Feistel Cipher

This can be described functionally as: L(i) = R(i-1)

R(i) = L(i-1) (+) g(K(i), R(i-1))

This can easily be reversed as seen in the above diagram, working backwards through the rounds and in practice link a number of these stages together (typically 16 rounds) to form the full cipher.

Reference-

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

QUESTIONS: -

Q1. Give an overview about Modern Private key ciphers.

Q2. Explain Practical Substitution-Permutation Networks.

Q3. What is S-Box? Explain its functionality.

Next, we will discuss more about Modular Arithmetic.

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