Shankersinh Vaghela Bapu Institute Of Technology.

IDEA

International Data Encryption Algorithm

History…

- IDEA is a **symmetric block cipher algorithm.**
- It was developed by **Xuejia Lai** and **James L. Massey.**

- Its patents are held by the Swiss company "Ascom-Tech AG".

Contd…

- It was meant to be a **replacement** for the **Data Encryption Standard.**
- IDEA was used in **Pretty Good Privacy (PGP) v2.0 .**
- It is developed at **ETH(Eidgenossische Technische Hochschule)** in **Zurich, Switzerland** in **1990**.

Basic idea about IDEA…

- Here Plain text is of 64 bit.
- Key is of 128 bit. And it is divided in 52 sub keys (how?? Thhat we will see in next slide.)
- Cipher text is also as same as plain text in size that is of 64 bit.
- Number of identical rounds are 8 where in each round 6 keys are used.
- Like this 48 keys and in last round another 4 keys (6 * 8 = 48 + 4 =52 total) are being used in both the encryption and decryption process.

Design issue

- The design philosophy behind the algorithm is one of “ mixing operation from different algebraic groups”
- Lets take a look which different operations are used.
    - 1) XOR
    - 2) Addition
    - 3) Multiplication

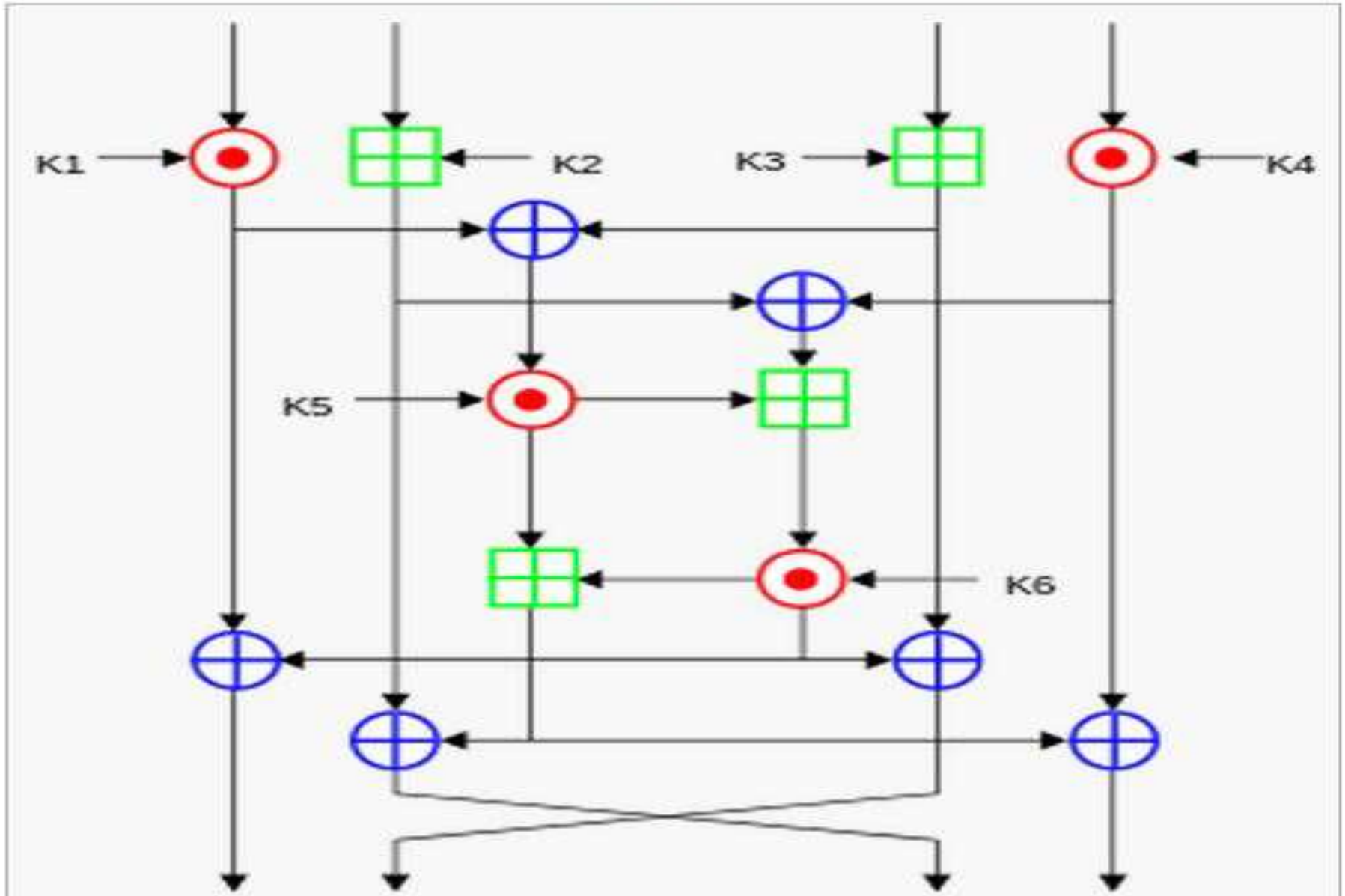
Key generation process

- First of all we will see how these 52 keys are generated.
- The 128 bit key is divided into 8 sub parts that is 16 bits each.
- Then the 128 bit key is cyclically shifted to the left by 25 position, so by doing this we will have one new 128 bit key.
- Now similarly as above it is divided into 8 sub blocks and will be used in next round.
- The same process is performed 9 times ans 56 keys are generated from which the first 52keys will be used.
- So likewise from K1 to K52 keys are generated.

Sequence of operation in one round

- 1) Multiply P1 and K1
- 2) Add P2 and second K2
- 3) Add P3 and third K3
- 4) Multiply P4 and K4
- 5) Step 1 $\oplus$ step 3
- 6) Step 2 $\oplus$ step 4
- 7) Multiply step 5 with K5

IDEA



An encryption round of IDEA

Sequence of operation in one round

- 8) Add result of step 6 and step 7
- 9) Multiply result of step 8 with K6.
- 10) Add result of step 7 and step 9.
- 11) XOR result of steps 1 and step 9.
- 12) XOR result of steps 3 and step 9.
- 13) XOR result of steps 2 and step 10.
- 14) XOR result of steps 4 and step 10.

- Same operations are performed in 8 rounds…

Sequence of operation in last round

- 1) Multiply P1 with K49.
- 2) Add P2 and K50.
- 3) Add P3 and K51.
- 4) Multiply P4 and K52.

Encyption

- First of all 64 bit plain text is divided into 4 16-bit parts and they are taken as an input in first round.
- At the end of the first encryption round four 16-bit values are produced which are used as input to the second encryption round
- The process is repeated in each of the subsequent 8 encryption rounds
- Note that in 9^{th} round we have to use only 4 key(K49, K50, K51,K52) and have to perform different operation as guided in previous slide.

Decryption

- The computational process used for decryption of the ciphertext is essentially the same as that used for encryption
- The only difference is that each of the 52 16-bit key sub-blocks used for decryption is the inverse of the key sub-block used during encryption
- Do remember that the sub blocks must be used in reverse order than of the encryption round.

Applications of IDEA

- Today, there are hundreds of IDEA-based security solutions available in many market areas, ranging from Financial Services, and Broadcasting to Government
- The IDEA algorithm can easily be combined in any encryption software. Data encryption can be used to protect data transmission and storage.
- Typical fields are:
  - Audio and video data for cable TV, video conferencing, distance learning
  - Sensitive financial and commercial data
  - Email via public networks
  - Smart cards

Hey all mature people please attention here:

Don't forget to go for vote on the day after tomorrow that is on 30th april... ☺

Heartly thank you for your time and attention…

Guided by:
Anand sir.

presented by:
Akshay (110750107020)
Akash (110750107005)
Saurabh (110750107021)