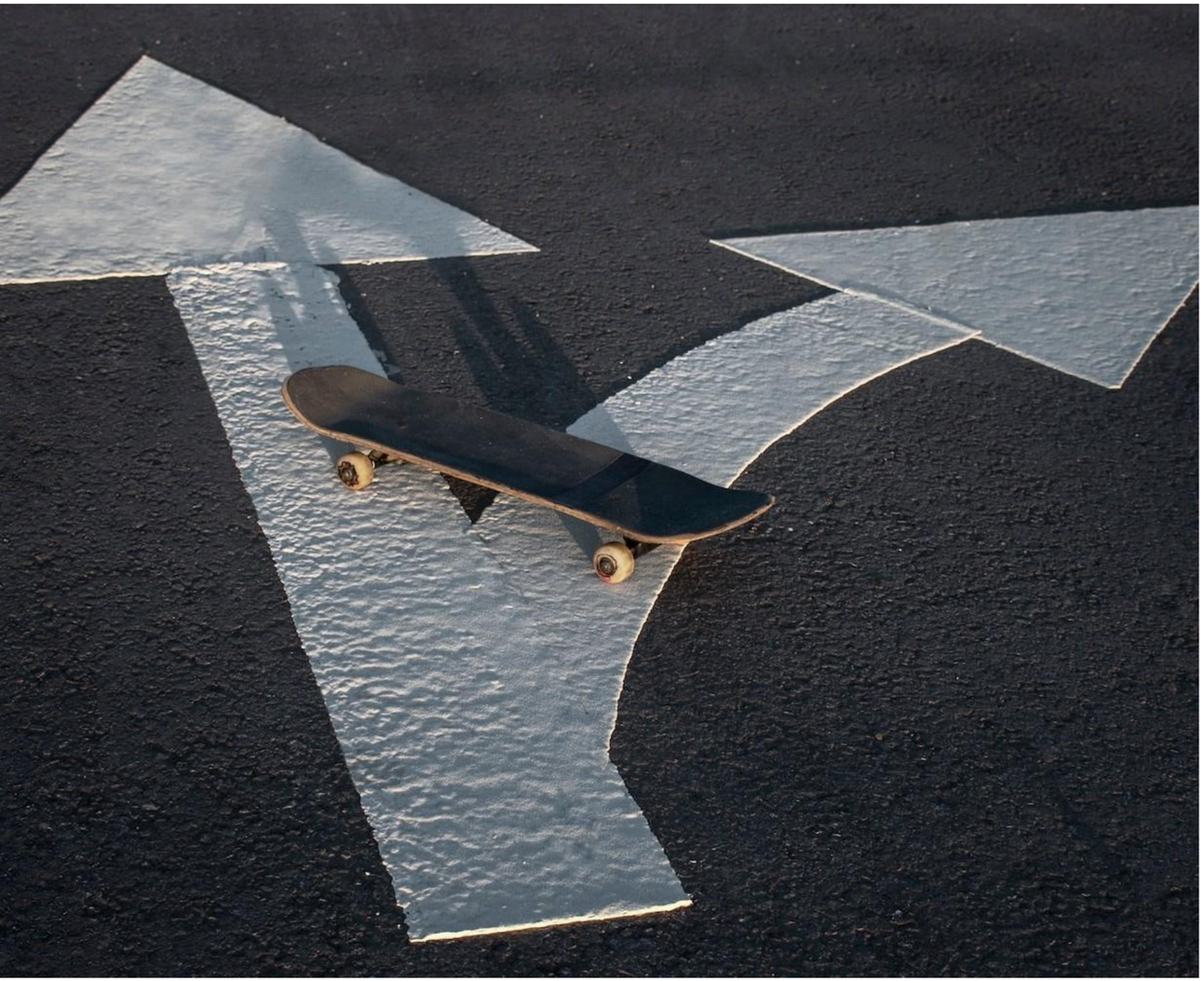


IDEA ENCRYPTION ALGORITHM

HISTORY OF IDEA

The **International Data Encryption Algorithm** (IDEA) was developed in 1991 as a **block cipher.** Its design was based on the **substitution-permutation network.** IDEA has been widely used in various applications due to its **strong security** features.

KEY FEATURES

IDEA is known for its **128-bit key length** and **highly secure encryption.** Its **complex arithmetic operations** make it resistant to **brute force attacks.** The algorithm also provides **confidentiality** and **integrity** of data.

ENCRYPTION PROCESS

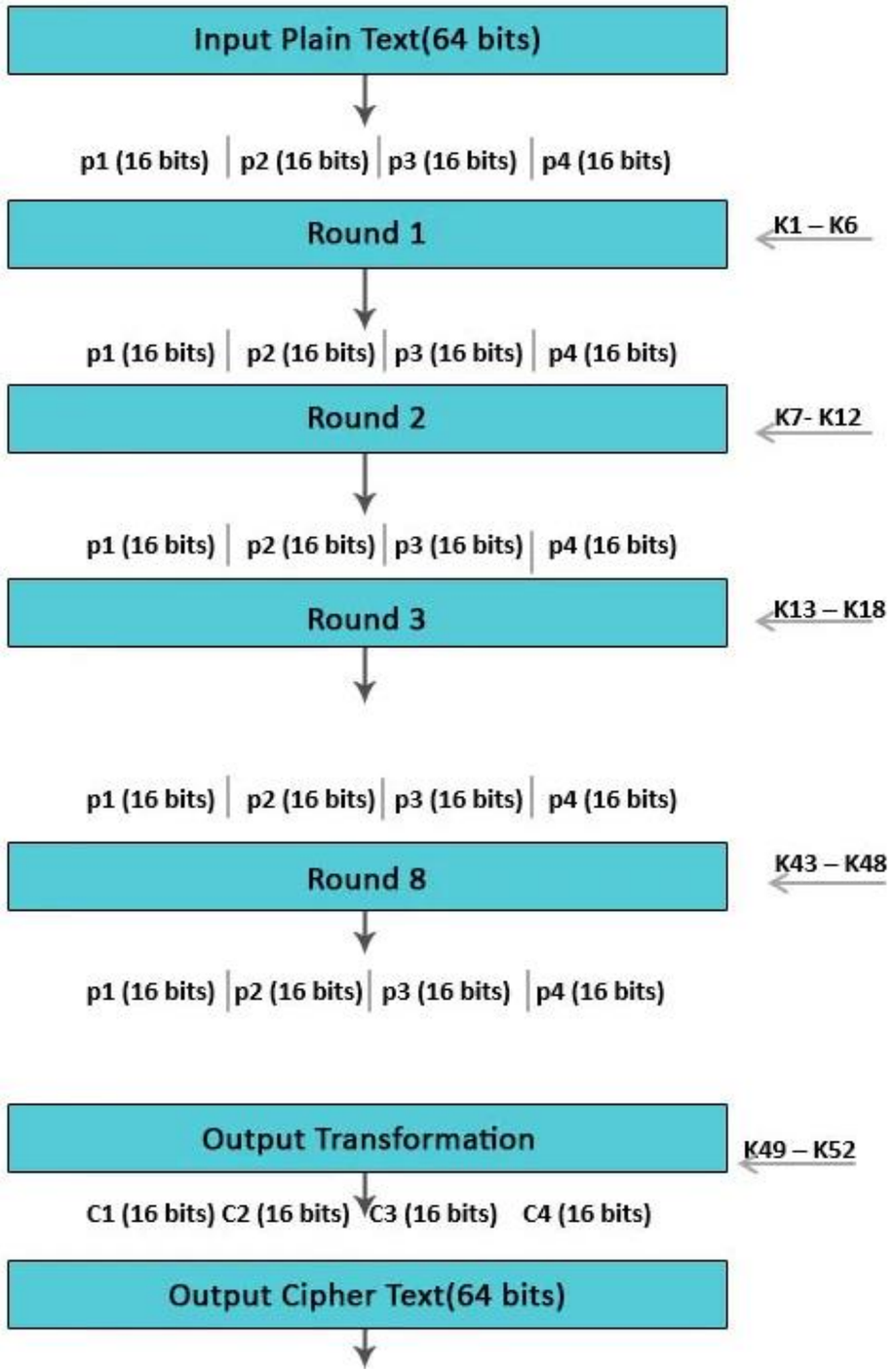
The **encryption process** involves **multiple rounds** of **substitution** and **permutation** operations. The **key scheduling** algorithm ensures the security of the encryption. IDEA's structure makes it **extremely difficult to decrypt** without the correct key.

ENCRYPTION PROCESS

- IDEA is a block ipher and it operates on **64 bit** plaintext and **128 bit** key. IDEA is reversible like DES that is, the equivalent algorithm can be used for encryption and decryption. IDEA needs both diffusion and confusion for encryption.

- The 64-bit plaintext is divided into four portions of **16 bit plaintext (P_1 to P_4).** These are input to the first round. There are **eight** such rounds.

- The key includes 128 bits. In each round, six sub-keys are produced from the original key, each of these sub-key includes 16 bits.

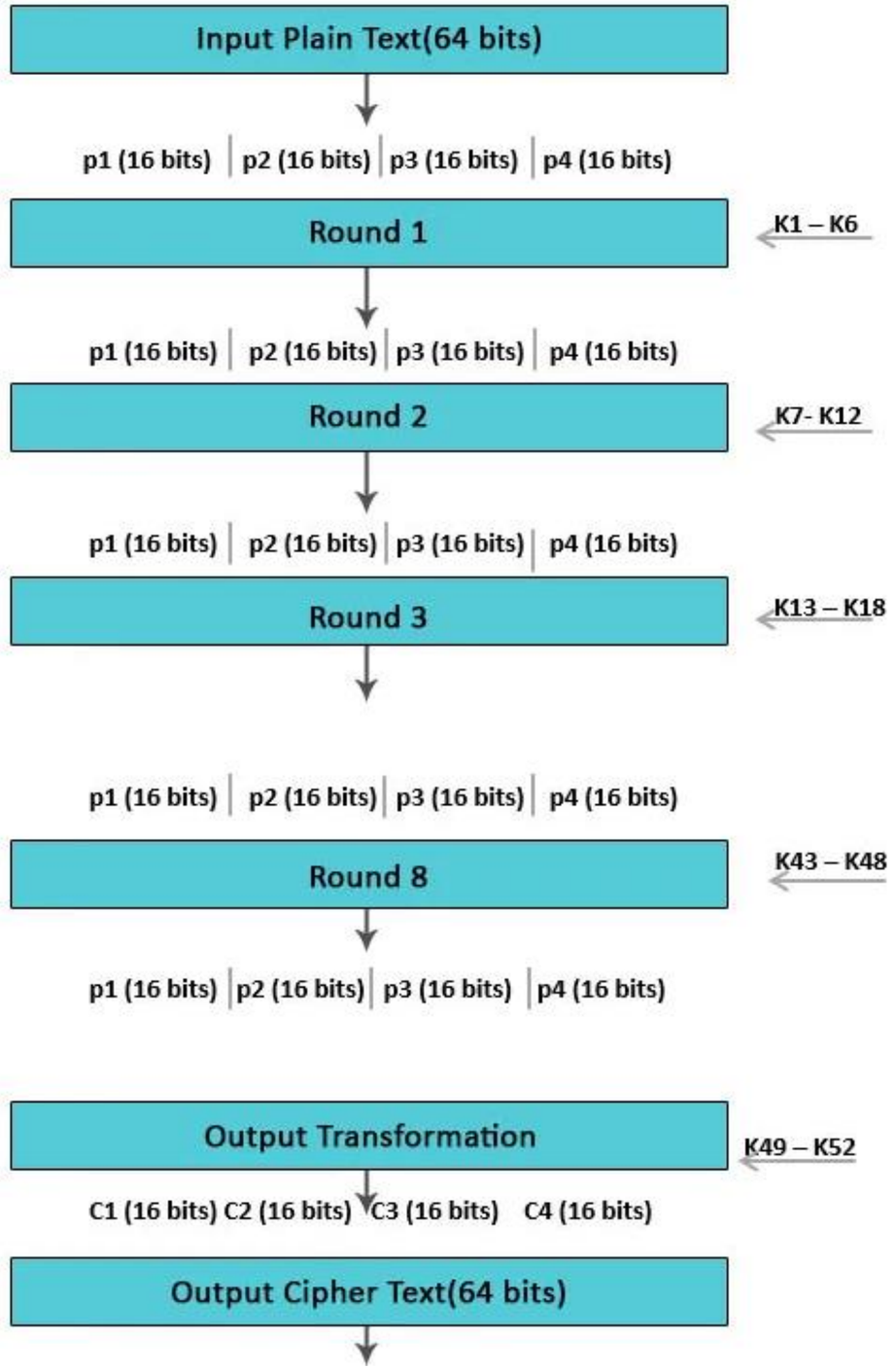


ENCRYPTION PROCESS

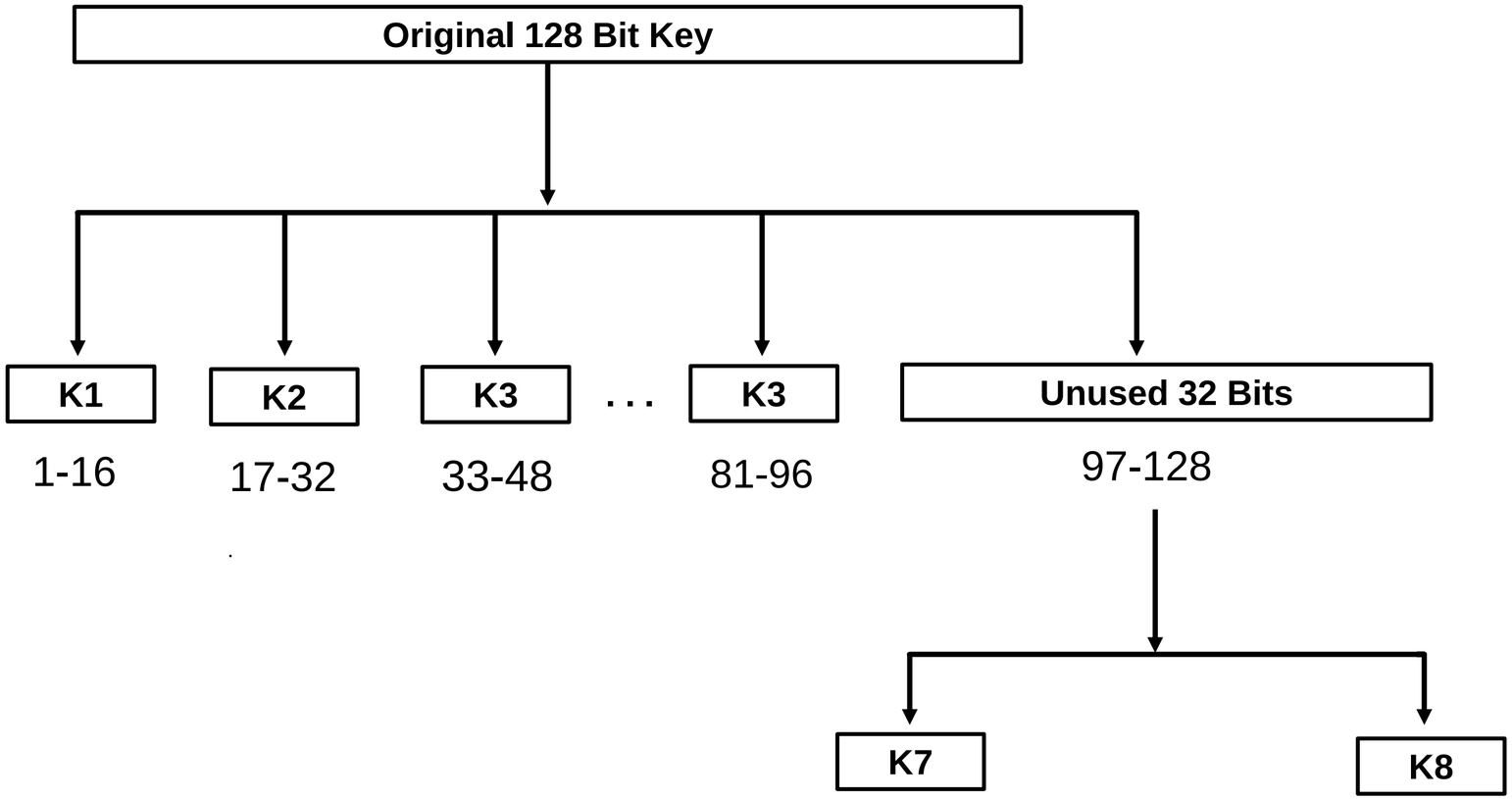
- For the first round it can have key **K1 to K6**, for second round it can have keys **K7 to K12** and finally the last round. The final step includes an output transformation, which needs four subkeys **(K49 to K52).**

- The final output is the output created by the output transformation step. The blocks C1 to C4 are linked to form the final output.

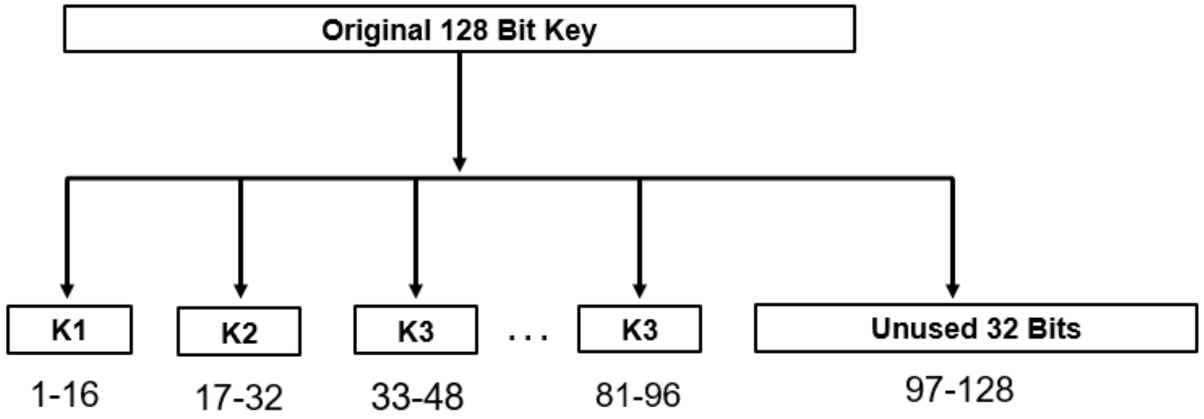
- **Rounds –** There are eight round in IDEA. Each round contains a sequence of operations on the four data blocks, utilizing six keys. The Add * and Multiply * in the following step of each round are not simple additions and multiplication but they are addition module 2^16 and multiplications modulo 2^16.

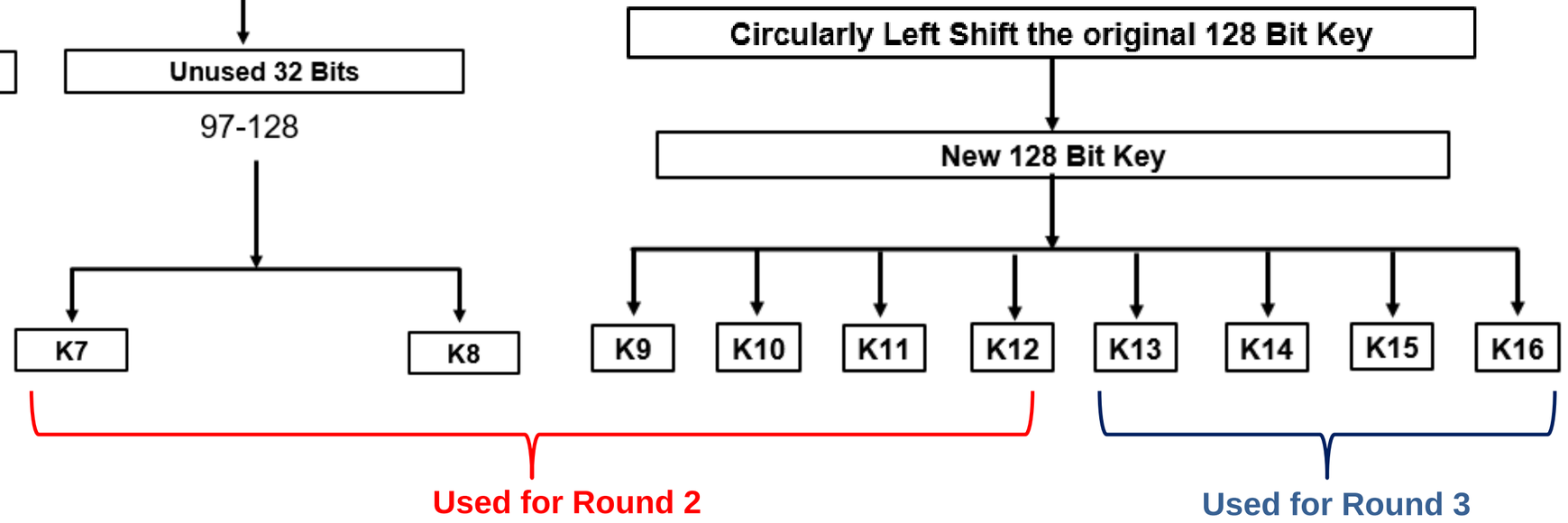


Key Expansion Process

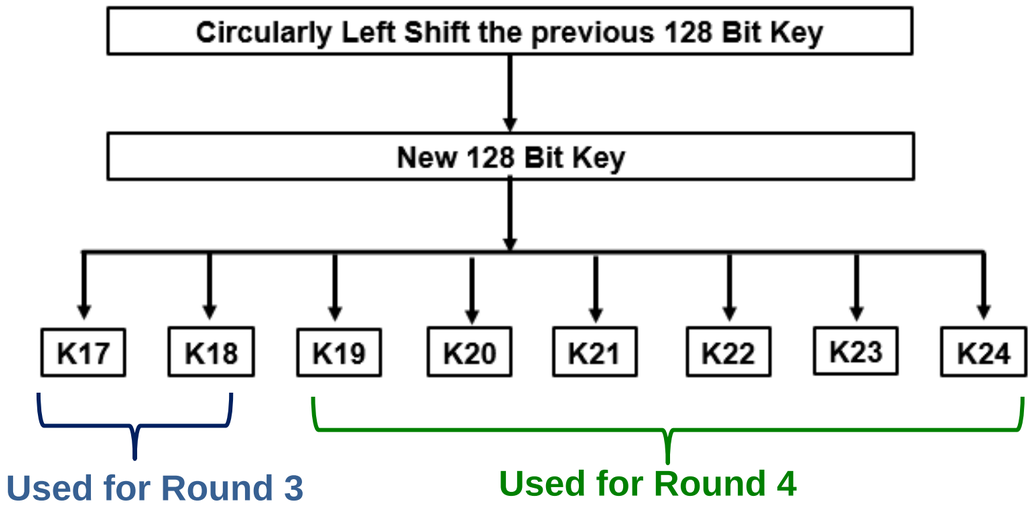


Key Expansion Process



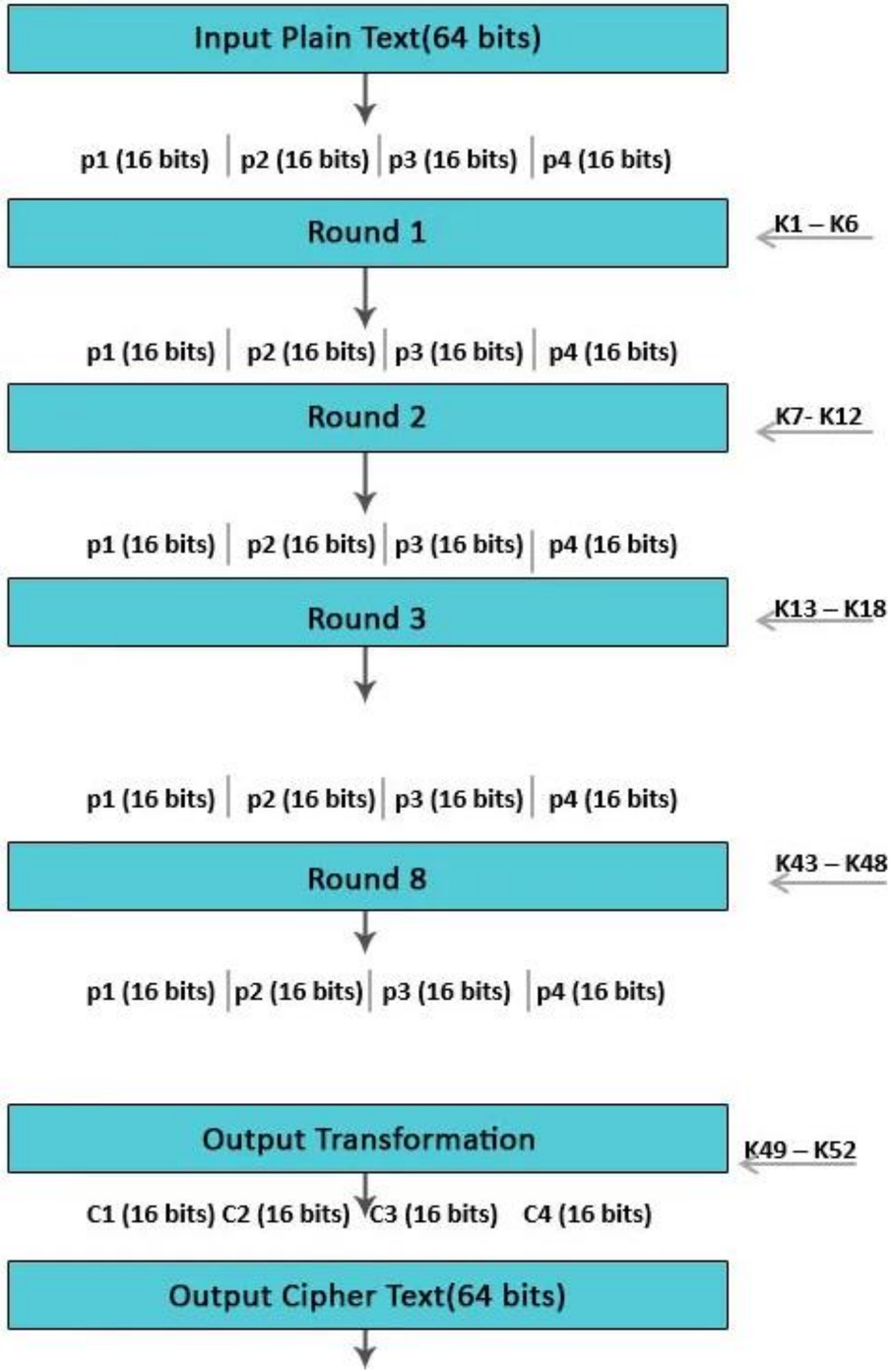


52 Subkey Generation



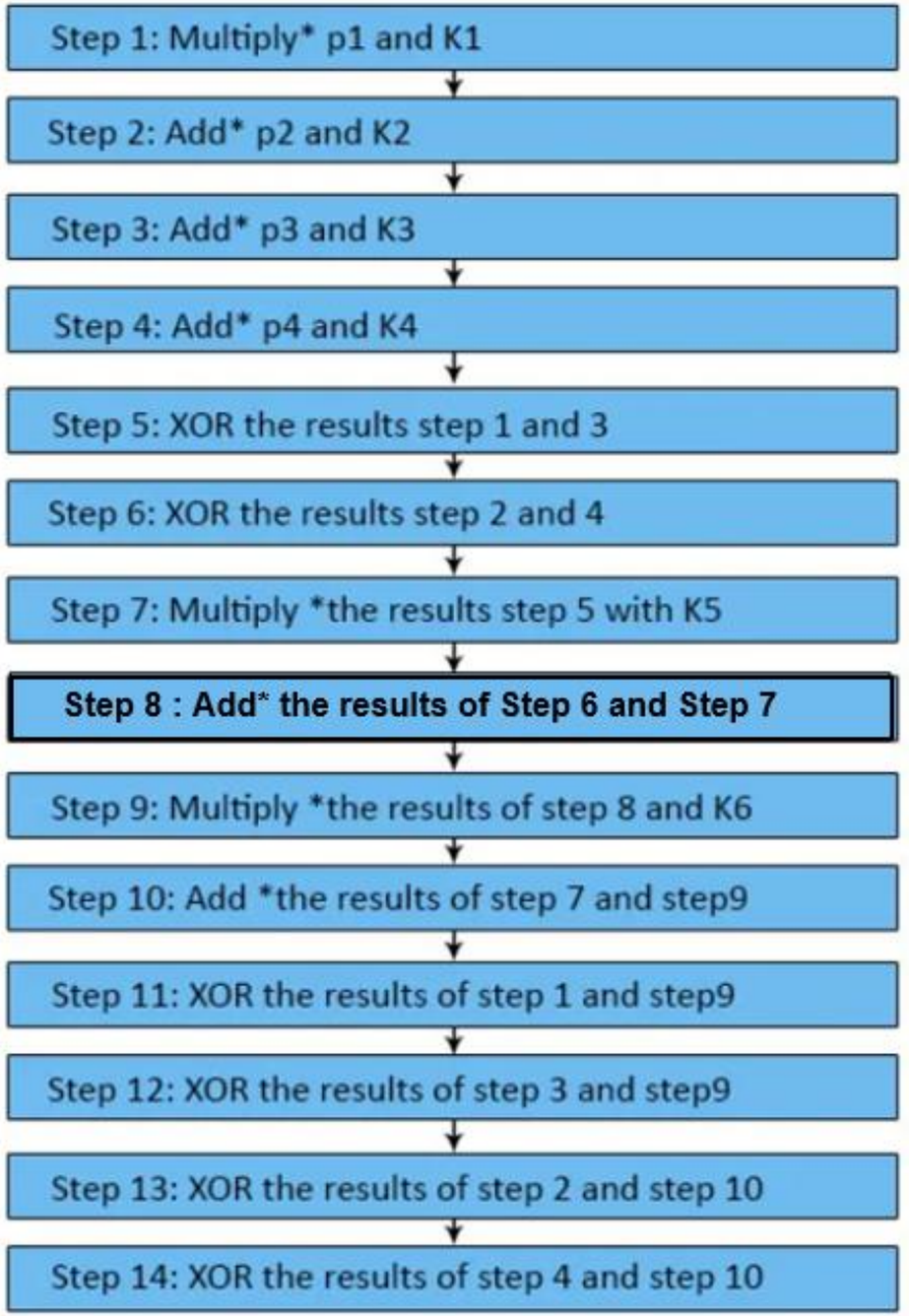
Encryption Process

- The 64-bit input plain text block is divided into 4 parts (16 bits each)
- Declare **p1 to p4**.
- Therefore, p1 to p4 will be the inputs for the initial round of the algorithm.
- There are **8 such rounds**.
- The key is made up of **128 bits**.
- In each round, **6 sub-keys** will be produced.
- Each one of the sub-keys includes **16 bits**.
- All these sub-keys will be put on the 4 input blocks p1 to p4.
- The last actions include Output Transformation, which usually benefits simply **4 sub-Keys.**
- The last result is 4 blocks of ciphertext C1 to C4 (each of 16 bits).
- They are mixed to create the last 64-bit ciphertext block.



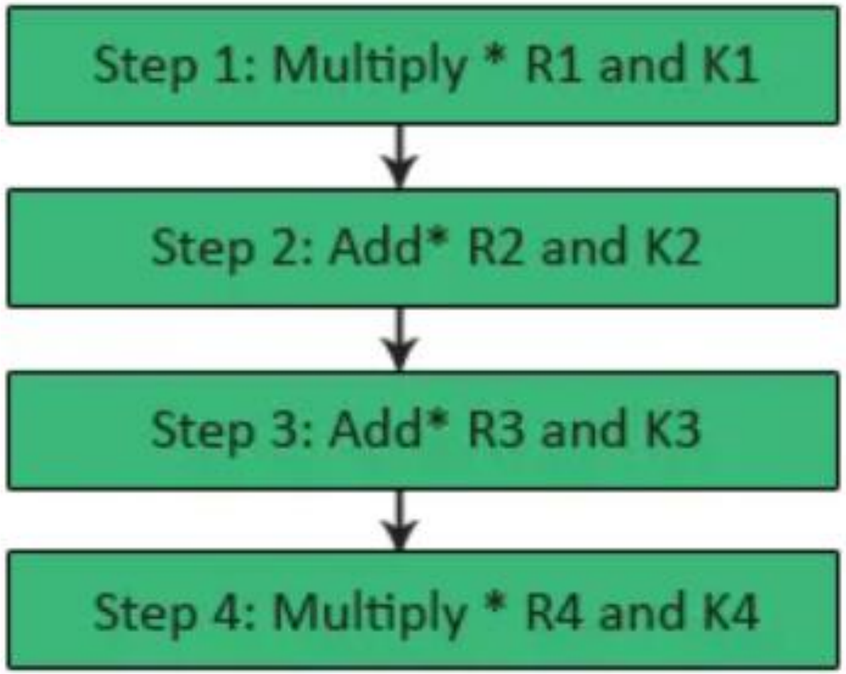
Detailed Single Round

- There are 8 rounds in IDEA.
- Every single requires several operations around the four data blocks applying 6 keys.
- These steps work in numerous mathematical activities.
- There are multiple *, add * & XOR procedures.
- Multiply * means multiplication modulo.
- Add* requires addition modulo.



Output Transformation

- It can be a one-time procedure.
- It requires places by the end of the 8th round.
- The Output transformation input is a 64-bit value divided into 4 sub-blocks (state R1 to R4 every among 16 bits).
- The four 16 bits Sub-keys (K1 to K4) are used here.
- The process of the outcome transformation can be as follows.



APPLICATIONS

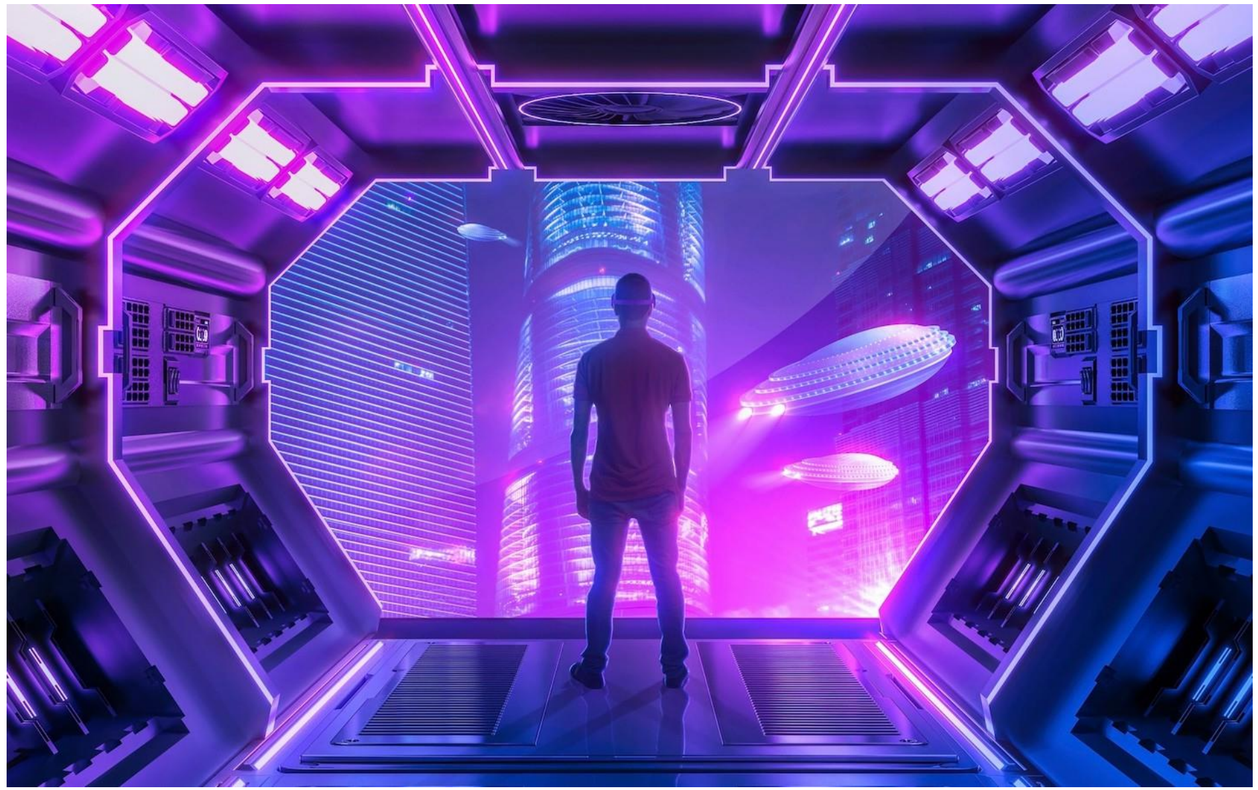
IDEA has been widely used in **secure communication** systems, **financial transactions**, and **data storage**. Its **strong encryption** capabilities make it suitable for **protecting sensitive information** in various domains.

CHALLENGES AND LIMITATIONS

While IDEA is a **powerful encryption algorithm**, it also faces **challenges** such as **key management** and **performance**. The **need for stronger encryption** in the face of advancing technology is also a consideration.

CRYPTANALYSIS OF IDEA

Several **cryptanalysis attempts** have been made to break IDEA's security. These efforts have highlighted the **strengths** and **weaknesses** of the algorithm, leading to **enhancements** and **modifications** to improve its security.



FUTURE DEVELOPMENTS

The future of IDEA lies in **further research** to enhance its **resilience** against **advanced attacks. Quantum computing** and **post-quantum cryptography** pose new challenges that require continuous**innovation** in encryption algorithms.

CRYPTOGRAPHIC STANDARDS

IDEA has been considered for **cryptographic standards** and has contributed to the development of **modern encryption algorithms**. Its impact on **cybersecurity** standards and protocols is significant.

SEC RIT BEST PRACTICES

Incorporating IDEA into **security best practices** involves **careful key management** and **regular updates** to address **vulnerabilities.** Understanding the **strengths and limitations** of IDEA is essential for its e ective implementation.

REAL-WORLD EXAMPLES

Real-world examples of IDEA's application in **secure messaging apps**, **secure file storage**, and **financial institutions** demonstrate its **effectiveness** in protecting sensitive data. These examples showcase IDEA's **relevance** in modern security systems.

CONCLUSION

In conclusion, the **IDEA Encryption Algorithm** continues to be a **cornerstone of secure communications** and **data protection.** It's **robust security features** and **historical significance** makes it a vital component of modern **cryptography**

Thanks!

Do you have any questions?

c.sridhar89@gmail.com
www.iamsridhariyer.com
youtube: @sridhariyer