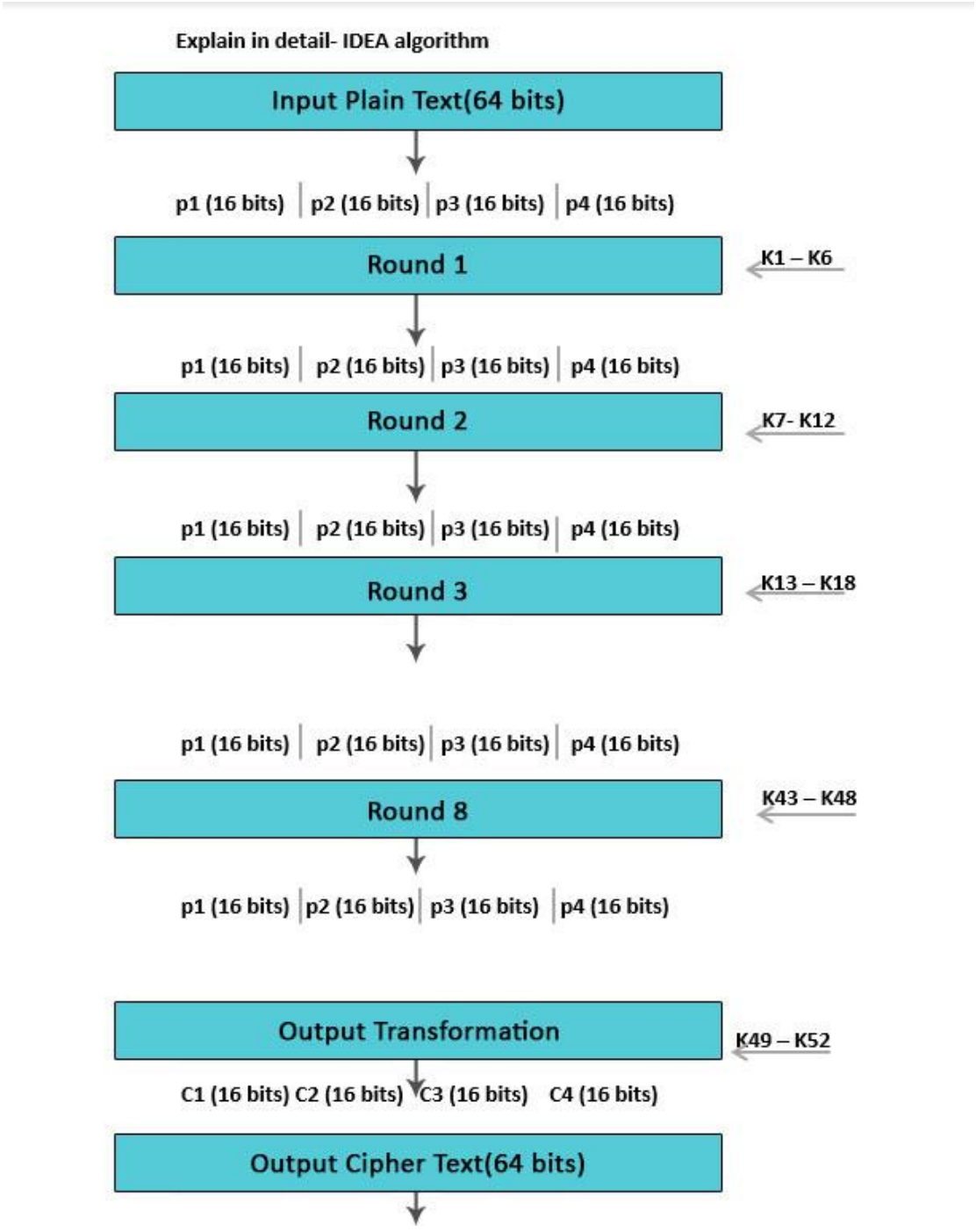
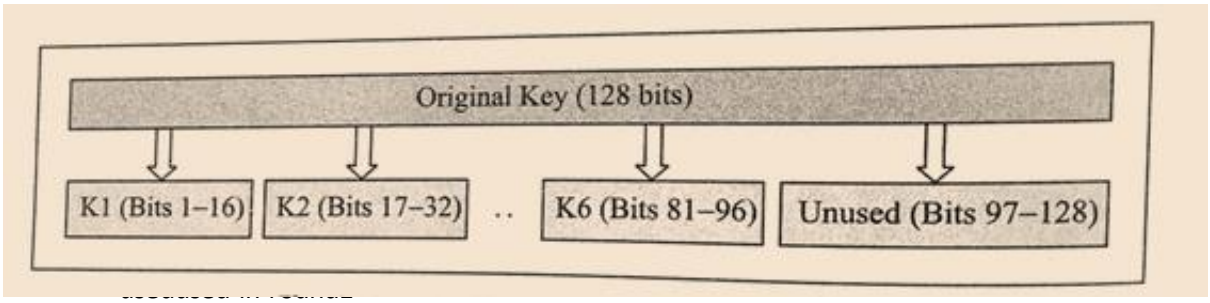
IDEA Algorithm

IDEA (International Data Encryption Algorithm) is an encryption algorithm. It is a symmetric block cipher that takes 64 bit as an input, 128-bit key and performs 8 identical rounds for encryption in which 6 different sub keys are used, and four keys are used for output transformation.



HOW TO GENERATE 52 SUB KEY



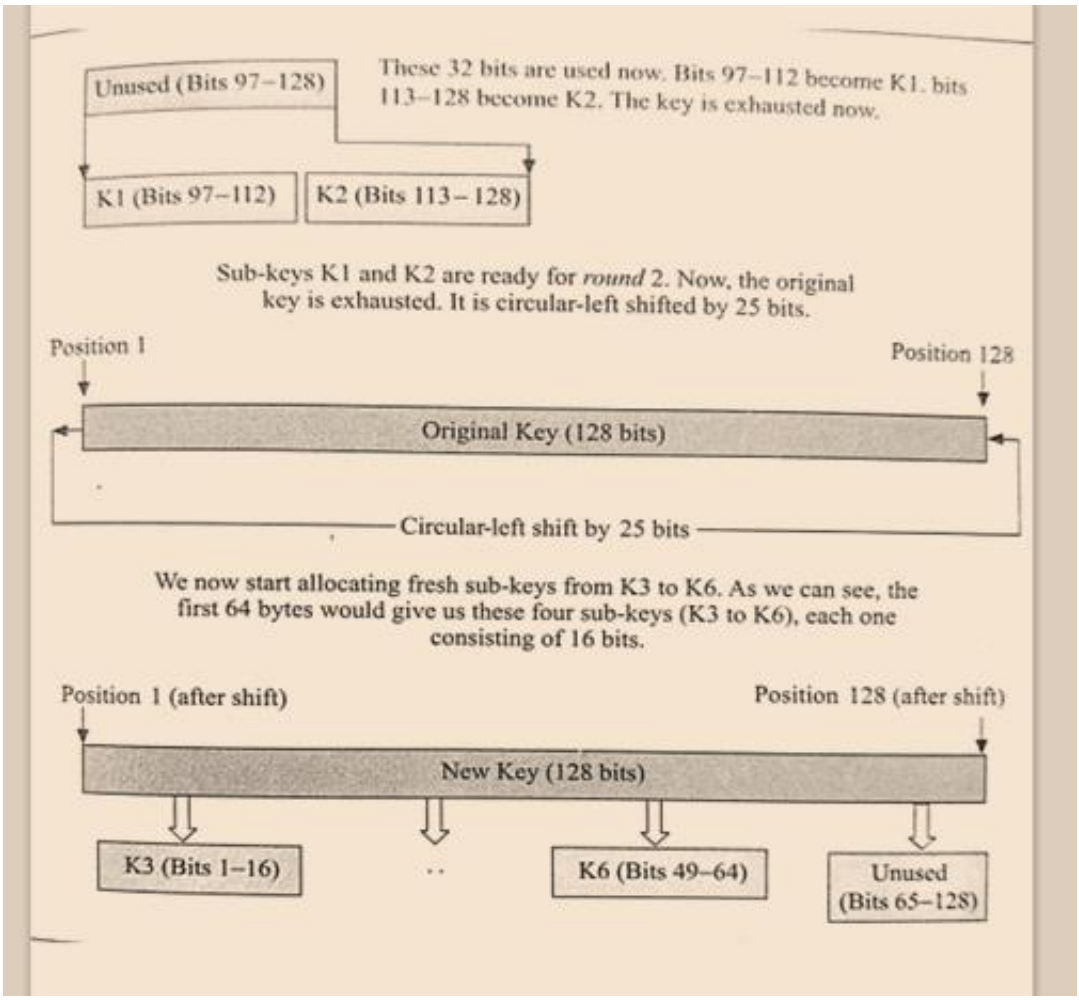
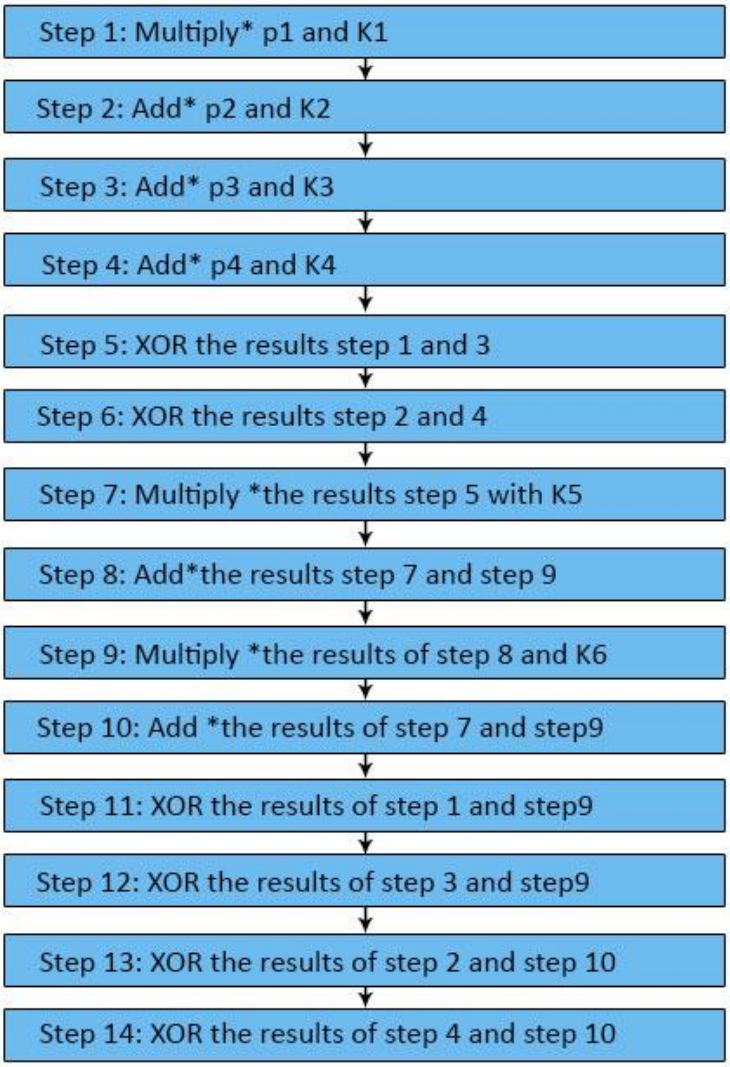


Table 3.4 Sub-key generation process for each *round*

Round	Details of the sub-key generation and use
1	Bit positions 1–96 of the initial 128-bit key would be used. This would give us 6 sub-keys K1 to K6 for Round 1. Key bits 97 to 128 are available for the next round.
2	Key bits 97 to 128 make up sub-keys K1 and K2 for this round. A 25-bit shift on the original key happens, as explained. Post this shifting; the first 64 bits are used as sub-keys K3 to K6 for this round. This leaves bits 65 to 128 unused for the next round.
3	Unused key bits 65 to 128 are used as sub-keys K1 to K4 of this round. Upon key exhaustion, another 25-bit shift happens, and bits 1 to 32 of the shifted key are used as sub-keys K5 and K6. This leaves bits 33 to 128 unused for the next round.
4	Bits 33 to 128 are used for this round, which is perfectly adequate. No bits are unused at this stage. After this, the current key is again shifted.
5	This is similar to Round 1. Bit positions 1–96 of the current 128-bit key would be used. This would give us 6 sub-keys K1 to K6 for Round 1. Key bits 97 to 128 are available for the next round.
6	Key bits 97 to 128 make up sub-keys K1 and K2 for this round. A 25-bit shift on the original key happens, as explained. Post this shifting; the first 64 bits are used as sub-keys K3 to K6 for this round. This leaves bits 65 to 128 unused for the next round.
7	Unused key bits 65 to 128 are used as sub-keys K1 to K4 of this round. Upon key exhaustion, another 25-bit shift happens, and bits 1 to 32 of the shifted key are used as sub-keys K5 and K6. This leaves bits 33 to 128 unused for the next round.
8	Bits 33 to 128 are used for this round, which is perfectly adequate. No bits are unused at this stage. After this, the current key is again shifted for the *Output Transformation* round.

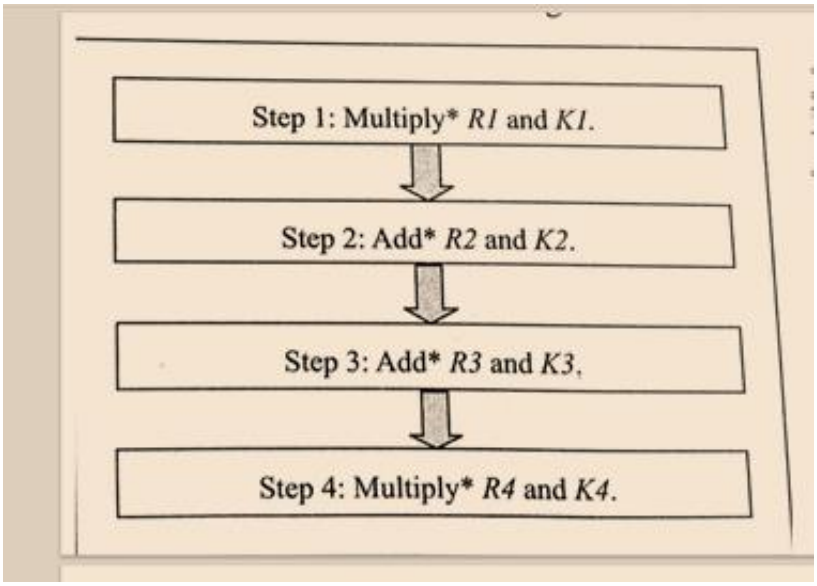
Single Round Information

- 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

Today, there are hundreds of IDEA-based security solutions available in many market areas, ranging from Financial Services, and Broadcasting to Government. IDEA is the name of a proven, secure, and universally applicable block encryption algorithm, which permits effective protection of transmitted and stored data against unauthorized access by third parties. The fundamental criteria for the development of IDEA were highest security requirements along with easy hardware and software implementation for fast execution.

The IDEA algorithm can easily be embedded 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, pay TV, video conferencing, distance learning, business TV, VoIP
– Sensitive financial and commercial data
– Email via public networks
– Transmission links via modem, router or ATM link, GSM technology
– Smart cards

Modes of operation

IDEA supports all modes of operation as described by NIST in its publication FIPS 81. A block cipher encrypts and decrypts plaintext in fixed-size-bit blocks (mostly 64 and 128 bit). For plaintext exceeding this fixed size, the simplest approach is to partition the plaintext into blocks of equal length and encrypt each separately. This method is named Electronic Code Book (ECB) mode. However, Electronic Code Book is not a good system to use with small block sizes (for example, smaller than 40 bits) and identical encryption modes. As ECB has disadvantages in most applications, other methods named modes have been created. They are Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Output Feedback (OFB) modes.

Conclusion

- IDEA may be a recognized cipher that many experts have examined for the previous 10 Sub-key creation for the round, each one of the 8 rounds utilizes 6 sub-keys (hence 8 * 6 = 48 sub-keys are essential for the rounds). The last result transformation benefits 4 sub-keys (i.e. 48 + 4 = 52 sub-keys total). From an input key 128 bits, all these 52 sub-keys will be produced years, as well as; however, no strike against five or higher of its 8.5 rounds has been found.
- Because of its toughness against cryptanalytic attacks and because of its inclusion in several well-known cryptographic deals, IDEA can be trusted. The Basic IDEA algorithm is definitely not, which can be likened for effectiveness or security with simple DES or AES versions. The Basic IDEA algorithm is intended to assist learners in being familiar with the IDEA algorithm by giving a version of IDEA that enables instances to get worked well manually and to offer a comparison of the technique of IDEA and the ways of DES and AES.