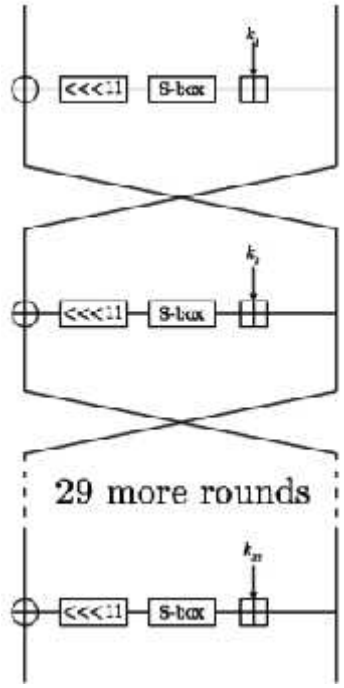
**Lucifer Block Cipher:**

In cryptography, **Lucifer** was the name given to several of the earliest civilian block ciphers, developed by Horst Feistel and his colleagues at IBM. LUCIFER uses a combination of Transposition and Substitution crypting as a starting point in decoding ciphers. One variant, described by Feistel in 1971uses a 48-bit key and operates on 48-bit blocks. The cipher is a Substitution-permutation network and uses two 4-bit S-boxes. The key selects which S-boxes are used. The execution of the cipher operating on 24-bits at a time, and also a sequential version operating on 8-bits at a time. Another variant uses a 64-bit key operating on a 32-bit block, using one addition mod 4 and a singular 4-bit S-box. The construction is designed to operate on 4 bits per clock cycle. This may be one of the smallest block-cipher implementations known. Feistel later described a stronger variant that uses a 128-bit key and operates on 128-bit blocks. Sorkin (1984) described a later Lucifer was a 16-round Feistel network, also on 128-bit blocks and 128-bit keys. This version is susceptible to differential cryptanalysis; for about half the keys, the cipher can be broken with 236 chosen plaintexts and 236 time complexity. IBM submitted the Feistel-network version of Lucifer as a candidate for the Data Encryption Standard. It became the DES after the National Security Agency reduced the cipher's key size to 56 bits, reduced the block size to 64 bits, and made the cipher resistant against differential cryptanalysis, which was at the time known only to IBM and the NSA.

**GOST Block Cipher:**

The GOST block cipher (Magma), is a Soviet and Russian government standard symmetric key block cipher with a block size of 64 bits. The GOST hash function is based on this cipher. Developed in the 1970s, the standard had been marked "Top Secret" and then downgraded to "Secret" in 1990. Shortly after the dissolution of the USSR, it was declassified and it was released to the public in 1994. GOST 28147 was a Soviet alternative to the United States standard algorithm, DES Thus, the two are very similar in structure.




GOST has a 64-bit block size and a key length of 256 bits. Its S-boxes can be secret, and they contain about 354 ($\log_2(16!^8)$) bits of secret information, so the effective key size can be increased to 610 bits; however, a chosen-key attack can recover the contents of the S-Boxes in approximately $2^{32}$ encryptions.

GOST is a Feistel network of 32 rounds. Its round function is very simple: add a 32-bit subkey modulo $2^{32}$, put the result through a layer of S-boxes, and rotate that result left by 11 bits. The result of that is the output of the round function. In the adjacent diagram, one line represents 32 bits.

The subkeys are chosen in a pre-specified order. The key schedule is very simple: break the 256-bit key into eight 32-bit subkeys, and each subkey is used four times in the algorithm; the first 24 rounds use the key words in order, the last 8 rounds use them in reverse order. The S-boxes accept a four-bit input and produce a four-bit output. The S-box substitution in the round function consists of eight 4 × 4 S-boxes. The S-boxes are implementation-dependent – parties that want to secure their communications using GOST must be using the same S-boxes. For extra security, the S-boxes can be kept secret.

**3 Way Block Cipher:**

In cryptography, **3-Way** is a block cipher designed in 1994 by Joan Daemen. It is closely related to BaseKing; the two are variants of the same general cipher technique.

3-Way has a block size of 96 bits, notably not a power of two such as the more common 64 or 128 bits. The key length is also 96 bits. The figure 96 arises from the use of three 32 bit words in the algorithm, from which also is derived the cipher's name. When 3-Way was invented, 96-bit keys and blocks were quite strong, but more recent ciphers have a 128-bit block, and few now have keys shorter than 128 bits.

3-Way is an 11-round substitution-permutation network. 3-Way is designed to be very efficient in a wide range of platforms from 8-bit processors to specialized hardware, and has some elegant mathematical features which enable nearly all the decryption to be done in exactly the same circuits as did the encryption.

**Crab Block Cipher:**

In cryptography, **Crab** is a block cipher proposed by Burt Kaliski and Matt Robshaw at the first Fast Software Encryption workshop in 1993. Not really intended for use, Crab was developed to demonstrate how ideas from hash functions could be used to create a fast cipher.

Crab has an unusually large block size of 8192 bits. Its creators suggested using an 80-bit key, but the cipher could use any key size. The authors didn't specify an actual key schedule, only that the key is used to generate two large sets of subkeys: a permutation of the numbers 0 through 255, and an array of 2048 32-bit numbers.

The block is divided into 256 32-bit sub-blocks, which are permuted at the beginning. Then the algorithm makes four passes over the data, each time applying one of four transformations adapted from MD5.