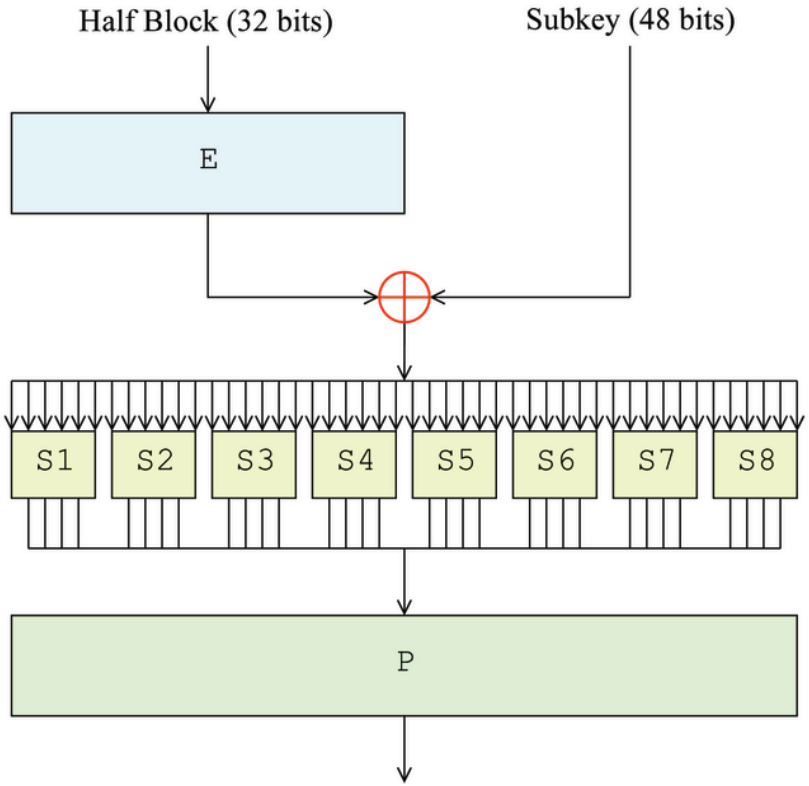
Data Encryption Standard



DES History

- The Data Encryption Standard is a US standard that provided confidentiality for financial transactions from 1970s till to the end of 1990s
- It was developed by IBM, based on ideas of Horst Feistel, and submitted to the National Bureau of Standards (the precursor of the National Institute of Standards and Technology) following an invitation to propose a candidate for the protection of **sensitive**, **unclassified** electronic data.
- After consulting with the National Security Agency (NSA), the NBS eventually selected a slightly modified version, which was published as an official Federal Information Processing Standard (FIPS) for the United States in 1977, with the number FIPS 46
- It quickly became an international standard, and enjoyed widespread deployment

Lucifer and Horst Feistel

- Lucifer was the name given to several of the earliest civilian block ciphers, developed by Horst Feistel and his colleagues at IBM — one version (named DTD-1) was in commercial use in the 1970s for electronic banking
- Horst Feistel (1915-1990) was a German-born cryptographer who worked on the design of ciphers at IBM, initiating research that gave birth to the Data Encryption Standard (DES) in the 1970s
- Feistel was one of the earliest non-government researchers to study the design and theory of block ciphers
- His ideas (S-boxes, round function) were based on Shannon's concepts of **confusion**, **diffusion**, and **mixing transformations**

Brief History

- However, there was also some controversy about it for several years
- The design philosophy of certain elements (S-boxes) was never explained (classified), and its key length was unnaturally short (56 bits) while it could have been 64 bits
- The NSA involvement was found suspicious by some
- There were conspiracy theories' about the DES having a "backdoor" for easy decryption [which was never proven to-day]
- Academic community also approached the DES with some caution, however, in the end, it significantly contributed to the development of modern cryptography for our communication and computing systems

Properties of DES

- The term "DES" actually refers to the standard, not just the algorithm, includes several methods about its usage (called modes)
- The encryption algorithm is sometimes called the Data Encryption Algorithm (DEA), however, both terms are used interchangeably
- It is a block cipher operating over binary data, with input (plaintext) and output (ciphertext) length of 64 bits
- The key length is 56 bits
- The cipher runs through 16 identical sub-operations, called rounds, each of which is using a 48-bit round key, a subset of the 56-bit key bits

Properties of DES

- Today, the single DES with a 56-bit key is no longer considered secure (discontinued as a US standard), since under a known text attack we can find the key by exhaustive search
- If a single encryption with a selected key can be performed in T seconds in a single computer, we can find the key (in the worst case) in $\frac{1}{n} \times 2^{56} \times T$ seconds by performing parallel searches with n computers

cycle	computers	total time
1 ms	1	2,284,900 years
	100	22,849 years
1 μs	1	2,285 years
	100	22.85 years
1 ns	1	2.28 years
	100	8.34 days