The Number of Rounds in Block Ciphers
NES/DOC/UIB/WP3/003/a

Lars R. Knudsen
University of Bergen

May 12, 2000

1 Design principle for block ciphers

The only generally accepted design principles for practical ciphers are the concepts of confusion and diffusion suggested by Shannon. Massey[1] interprets Shannon's concepts of confusion and diffusion[3] as follows *Confusion:* "The ciphertext statistics should depend on the plaintext statistics in a manner too complicated to be exploited by the cryptanalyst". *Diffusion:* "Each digit of the plaintext and each digit of the secret key should influence many digits of the ciphertext". These two design principles are very general and informal. Shannon also discusses two other more specific design principles. The first is to make the security of the system reducible to some known difficult problem. This principle has been used widely in the design of public-key systems, but not in secret-key ciphers. Shannon's second principle is to make the system secure against all known attacks, which is still the best known design principle for secret-key ciphers today.

Most often confusion is added to a block cipher in terms of some well-chosen S-boxes. Diffusion is most often implemented by means of some linear transformation. A typical product cipher, a term invented also by Shannon, uses a mix of S-boxes and linear transformations. By repeating a substitution layer and a linear transformation sufficiently many times one hopes to obtain a strong cipher.

There have been many suggestions in the past of more specific design principles, e.g. completeness, strict avalanche criterion, see [2, page 277-278].

However a specific cryptographic design principle should not be overvalued. Design principles should be seen as "guidelines" in the construction of ciphers, evolved from years of experience, and as necessary, but *not* sufficient requirements. There are many examples of this in the history of cryptography.

Design principle for block ciphers

To our knowledge there exist no theory on the number of rounds a block cipher should run in general.

Let $E_K(\cdot)$ be an n-bit iterated block cipher using a k-bit key K. Assume that the key K is expanded to r round-keys $K_1, \ldots, K_r$ in some key-scheduling

algorithm. Let C_0 be a plaintext block and define for $i = 1, \ldots, r$

$$C_i = F(C_{i-1}, K_i).$$

C_r is then the ciphertext. F is assumed to contain a *confusion stage* and a *diffusion stage*.

By a confusion stage we mean the application (possibly multiple applications) of some functions $g : \{0,1\}^s \to \{0,1\}^t$, for which any linear combination of the t bits in the output cannot be expressed as a linear function of some of the s input bits. By a diffusion stage we mean the application (possibly multiple applications) of some functions $h : \{0,1\}^u \to \{0,1\}^v$, which can be linear.

In the following we shall give a guideline for the number of rounds for a particular block cipher. For this we need the minimum word size, w in the inputs to the confusion stage overall in the cipher, that is, the number of bits in the smallest subblocks processed in the confusion stage. Also, we shall distinguish between the cases where the block cipher processes the entire block of n bits in one round and the cases where it processes only parts of a block in one round. We let d denote the maximum number of rounds it takes for one w-bit word to be input to a confusion stage. In the well-known Feistel ciphers $d = 2$, since only half the block is modified in each round.

Design Principle *Let r be the number of rounds for an iterated block cipher $E_K(\cdot)$ with block size n. Let w be the minimum word size input to the confusion stage overall in the cipher. Also let d be the maximum number of rounds it takes for one word to be input to a confusion stage. Then*

$$r \geq dn/w.$$

With this minimum number of rounds r one is guaranteed that each w-bit word has been input to a confusion stage r/d times. Assume that each confusion stage adds at least w bits of "uncertainty" to the intermediate ciphertext. Then the ciphertext after r rounds "has been added" at least wr/d bits of "uncertainty". With $r = dn/w$ as above $wr/d = n$ which is the maximum "uncertainty" for an n-bit block.

This is only a rough guideline in the selection of the number of rounds, e.g., since the influence of the diffusion layer has been totally ignored in these estimates.

However, what speaks in favor of our design principle is that, for all the block ciphers of Table 1, for which our minimum number of rounds is larger than the actual number of rounds weaknesses and/or attacks have been presented. In addition, for the block ciphers meeting our minimum number of rounds, reduced-round versions have been shown to be weak.

1.1 AES candidates

In the following we consider the final five candidates for the AES.

Algorithm	Actual no. of rounds	Our minimum
DES	16	21
Blowfish	16	16
FEAL	N	16
GOST	32	32
IDEA	8	8
LOKI'91	16	16
RC5	12	26
SAFER K	6	8
SKIPJACK	32	32

Table 1: The design principle used on some older ciphers.

Serpent: This is a classical SP-network, where operations are nibble-oriented, and each nibble is input to an S-box in every round. Here $n = 128$, $d = 1$, and $w = 4$.

Rijndael: This is also an SP-network, where operations are byte-oriented and each byte is input to an S-box in every round. Thus, $n = 128$, $d = 1$, and $w = 8$.

Twofish: This can be seen as two "parallel" Feistel-networks, where the outputs of each round function are combined. In each round, half the block is input to the confusion stage, and the S-boxes are 8-bit S-boxes. Thus, $n = 128$, $d = 2$, and $w = 8$.

MARS: This is a type-3 Feistel network where in each round one 32-bit word is used to update the 3 other 32-bit words. In each round a 9×32 S-box is applied, a keyed multiplication modulo 2^{32}, and two data-dependent rotations. However, MARS does not fall directly into the category of iterated ciphers we are considering here. If we view the S-box as the confusion stage and the rest as the diffusion stage, we get $n = 128, d = 4, w = 9$. On the other hand, if we consider the data-dependent rotations as part of the confusion stage we get $n = 128, d = 4, w = 19$. Note that multiplication by a keyed constant is a linear function.

RC6: This can be seen as two Feistel-networks which are combined through data-dependent rotations over the blocks together with a 32-bit multiplication function. Like MARS, RC6 does not fall directly into our category of ciphers. If we consider the multiplication function as part of the diffusion stage we get $n = 128, d = 2, w = 5$. On the other hand, if we consider the multiplication as part of the confusion stage we get $n = 128, d = 2, w = 32$.

Table 2 lists the number of rounds of three of the five final candidates together with the number of rounds suggested by the design principle. In these estimates we have not considered the confusion introduced by mixing group operations.

A design principle in block ciphers must be seen as a guideline. There is no guarantee that a block cipher safisfying our principle is a secure block cipher nor that a block cipher not safisfying our principle can be broken in any way.

Algorithm	Actual no. of rounds	Our minimum
Serpent	32	32
Rijndael	10	16
Twofish	16	32
MARS	32	?
RC6	20	?

Table 2: The design principle used on the five AES-finalists.

In fact, it is very easy to construct example ciphers illustrating these points. On the other hand it is remarkable how well the principle fits on older block ciphers and the best known attacks on these, re: Table 1.

References

[1] J.L. Massey. Cryptography: Fundamentals and applications. Copies of transparencies, Advanced Technology Seminars, 1993.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.

[3] C.E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.