DEAL - A 128-bit Block Cipher

Lars R. Knudsen

February 21, 1998

Abstract

We propose a new block cipher, DEAL, based on the DES (DEA). DEAL has a block size of 128 bits and allows for three key sizes of 128, 192, and 256 bits respectively. Our proposal has several advantages to other schemes: because of the large blocks, the problem of the "matching ciphertext attacks" is made small, and the encryption rate is similar to that of triple-DES. We conjecture that the most realistic (or the least unrealistic) attack on all versions of DEAL is an exhaustive search for the keys. We have suggested ANSI to include DEAL in the ANSI standard X9.52. We also suggest DEAL as a candidate for the NIST AES standard.

1 Introduction

The DES (or DEA) [15] is a 64-bit block cipher taking a 64-bit key, of which 56 bits are effective. It is an iterated 16-round cipher, where the ciphertext is processed by applying a round function iteratively to the plaintext. The DES has a so-called *Feistel structure*: in each round one half of the ciphertext is fed through a non-linear function, and the output XORed to the other half of the ciphertext, after which the two halves are swapped.

The key size of the DES has become too small for today's applications. Wiener [20] showed that at the cost of about one million US$ it is possible to construct a dedicated hardware device, capable of performing an exhaustive search of a DES key in expected time only 3.5 hours. Also, recently it was demonstrated that even in software a 56-bit key does not provide sufficient protection, when a DES key was found by exhaustive search using implementations distributed on the Internet.

However, the problem of the small key size was pointed out already shortly after the publication of the DES [6]. Therefore, often the DES is used in a triple encryption scheme, where a plaintext is encrypted thrice with 3 independent keys, called triple-DES. In another variant, called two-key triple DES, the plaintext is first encrypted with a key $K1$, then decrypted with a key $K2$, and finally encrypted again with key $K1$ [18]. However, the block size of 64 bits makes these proposals vulnerable to the *matching ciphertext attack*, which is based on the fact that for most modes of operations for the DES [16] after the encryption of 2^{33} blocks, equal ciphertext blocks can be expected and information is leaked about the plaintexts [5, 9, 13]. Also, triple-DES with three independent keys is vulnerable to a related-key attack [7] with a running time about the same as the time of an exhaustive search over one DES-key.

The American National Standards Institute (ANSI) committee X9.F.1 is working on adopting a suite of modes for triple encryption with the DES [21]. One of these modes is the Triple DES Cipher Block Chaining (TCBC) mode, where the feedback block is the ciphertext block after 3 DES encryptions, also called the *outer-CBC* mode. However, this mode is vulnerable to the matching ciphertext attack. Therefore it has been suggested to use triple-DES in a ciphertext block chaining mode with internal feedback, also called the *inner-CBC* mode, where the feedback is done after each single DES encryption. Although this mode is not as vulnerable to the matching ciphertext attack, efficient key-recovery attacks can be mounted running in time much less that one would expect for a triple encryption scheme [1].

In [5, 4] Coppersmith, Johnson, and Matyas propose the *CBC with OFB Masking* (CBCM) mode of operation for triple-DES. Wagner [5] cryptanalysed an early proposal, which led to the current design, where only 2^{20} values are allowed for one of the two initial values. The CBCM is not vulnerable to the matching ciphertext attack and the level of security is a conjectured 2^{80}. The disadvantage of the proposal is, that it uses 4 DES encryptions using three different DES keys to encrypt one 64-bit plaintext block. Recently, Biham and Knudsen showed that the DES used in the CBCM mode is vulnerable to a chosen ciphertext attack, which uses a chosen ciphertext consisting of 2^{65} blocks with time complexity 2^{58} [2].

Our proposal is an r-round Feistel cipher, which uses the DES in the round function. The result is a 128-bit block cipher with $r \cdot 64$ bits of round keys, which are derived from a key schedule algorithm. The key schedule is designed to accept keys of three different lengths, namely 128, 192, and 256 bits. For the first two key sizes, we recommend to use $r = 6$ and for 256 bit keys to use $r = 8$. Later in the paper we explain why we recommend $r \geq 6$. If the parity bits of each key byte is not used for encryption, as is the situation for the DES, the effective key lengths are reduced to 112, 168, and 224 bits respectively. Still, an exhaustive search for the key is clearly infeasible in any of the variants, see e.g., [3] for discussions about key sizes. Also, the matching ciphertext attack needs an input of about 2^{64} ciphertext blocks to succeed. Our proposal is as fast as triple-DES in that it uses six encryptions to encrypt two 64-bit plaintext blocks and moreover, it can be implemented using existing DES implementations.

The National Institute of Standards and Technology (NIST) recently announced that they intend to standardize a new encryption algorithm, the Advanced Encryption Standard, as a replacement for the DES [14]. NIST realises that it will be several years before the AES will be ready and that they intend to recognize the "Triple DES algorithm once it is approved as an ANSI standard" [14], which makes the ANSI initiative even more important.

2 DEAL

DEAL (Data Encryption Algorithm with Larger blocks) is a 128-bit block cipher with a choice of 128-bit, 192-bit, and 256-bit keys, hereafter denoted DEAL-128, DEAL-192, and DEAL-256, respectively. All versions can be used in all four standard modes of the DES [16]. We begin by describing how DEAL works in the ECB mode. Let $C = E_B(A)$ denote the encrypted value of 64-bit A using the DES with key B and let $Y = EA_Z(X)$ denote the encryption of 128-bit X using DEAL with key Z. The plaintext P is divided into blocks P_i of 128 bits each, $P = P_1, P_2, \ldots, P_n$. The key schedule takes the key K and returns r DES keys RK_i for $i = 1, \ldots, r$, as described later. Let X^L and X^R denote the left respectively right halves of X. The ciphertexts are computed as follows. Set $X_0^L = P_i^L$, $X_0^R = P_i^R$ and compute for $j = 1, \ldots, r$

$$X_j^L = E_{RK_j}(X_{j-1}^L) \oplus X_{j-1}^R \quad (1)$$

$$X_j^R = X_{j-1}^L. \quad (2)$$

Set $C_i = X_r^L \| X_r^R$. See Fig. 1 for one round of DEAL. For DEAL-128 and DEAL-192 we

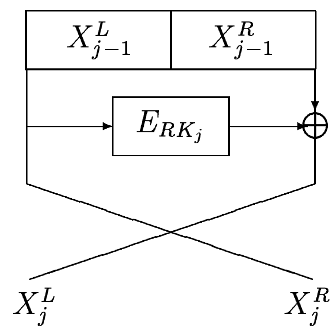

Figure 1: One round of DEAL.

suggest to use 6 rounds, that is $r = 6$. However, as we will see later, this may not be sufficient for DEAL-256 for which we suggest to use 8 rounds, $r = 8$. We imagine that the version with 256-bit keys is used only when very strong encryption is required.

Note that the swapping of the halves in the last round of DEAL is *not* omitted. The reason for this is: the right half of the ciphertext C_i is not encrypted in the last round of the ith encryption, and only the left half of the input to the $i + 1$st encryption, that is $C_i \oplus P_{i+1}$, is encrypted in the first round. Thus, the right half of C_i remains unencrypted for two rounds. This might give an attacker room to play, since the cipher consists of only six or eight rounds. Note that a similar property holds for the DES when used in the CBC mode. However, since the DES has 16 rounds, this seems to be harder to exploit. Let us note that the swapping of the halves in the last round has no effect on the security of the block cipher when used in the ECB mode.

The CBC mode works as specified in [16]. That is, let the 128-bit plaintext blocks be denoted $P_1, P_2, \ldots, P_n$ and denote by $C_1, C_2, \ldots, C_n$ the corresponding ciphertext blocks. Then

$$C_i = EA_K(C_{i-1} \oplus P_i),$$

where C_0 is an initial value.

In the DES an initial permutation IP is first applied to the plaintext and similarly, before output, the ciphertext is fed through IP^{-1}, the inverse of IP. It is possible to speed up an implementation of DEAL by removing these initial and final permutations from the DES implementation. It is an easy exercise to show that to get a correct implementation of DEAL, IP must be applied to both plaintext halves before encryption and IP^{-1} must be applied to both ciphertext halves.

The key schedule of DEAL takes as input s DES keys, $K_1, \ldots, K_s$, for $s = 2, 3, 4$, each K_i of 64 bits (including the 8 parity bits, the most significant bit of every byte) and returns r DES keys, RK_i. We use a general method which applies to all three key sizes. First expand the s keys to r keys, by repetition, and XOR the keys with a new constant for every repetition. Encrypt the expanded list of keys using the DES in CBC mode with a fixed key and with the initial value set to zero. The resulting ciphertext blocks form the subkeys RK_i. In the following we give the precise definition of each of the three key schedules, where $K = 0x0123456789abcdef_x$ (hex notation) is a fixed DES-key.

In DEAL-128 the subkeys are generated as follows:

$$
\begin{aligned}
RK_1 &= E_K(K_1), \\
RK_2 &= E_K(K_2 \oplus RK_1), \\
RK_3 &= E_K(K_1 \oplus \langle 1 \rangle \oplus RK_2), \\
RK_4 &= E_K(K_2 \oplus \langle 2 \rangle \oplus RK_3), \\
RK_5 &= E_K(K_1 \oplus \langle 4 \rangle \oplus RK_4), \\
RK_6 &= E_K(K_2 \oplus \langle 8 \rangle \oplus RK_5).
\end{aligned}
$$

where $\langle i \rangle$ denotes the usual representation of the integer i as a bit string.

In DEAL-192 the subkeys are generated as follows:

$$
\begin{aligned}
RK_1 &= E_K(K_1), \\
RK_2 &= E_K(K_2 \oplus RK_1), \\
RK_3 &= E_K(K_3 \oplus RK_2), \\
RK_4 &= E_K(K_1 \oplus \langle 1 \rangle \oplus RK_3), \\
RK_5 &= E_K(K_2 \oplus \langle 2 \rangle \oplus RK_4), \\
RK_6 &= E_K(K_3 \oplus \langle 4 \rangle \oplus RK_5).
\end{aligned}
$$

These versions of the key schedule require 6 DES key schedules and 6 DES encryptions with a fixed key. The subkeys have to be computed only once if they are subsequently stored.

In DEAL-256 the subkeys are generated as follows:

$$
RK_1 = E_K(K_1),
$$

$$
\begin{aligned}
RK_2 &= E_K(K_2 \oplus RK_1),\\
RK_3 &= E_K(K_3 \oplus RK_2),\\
RK_4 &= E_K(K_4 \oplus RK_3),\\
RK_5 &= E_K(K_1 \oplus \langle 1 \rangle \oplus RK_4),\\
RK_6 &= E_K(K_2 \oplus \langle 2 \rangle \oplus RK_5),\\
RK_7 &= E_K(K_3 \oplus \langle 4 \rangle \oplus RK_6),\\
RK_8 &= E_K(K_4 \oplus \langle 8 \rangle \oplus RK_7).
\end{aligned}
$$

This version requires 8 DES key schedules and 8 DES encryptions with a fixed key.

Note that for all versions of the key schedule the 64-bit quantities RK_i are used as DES-keys, therefore the parity bits of RK_i are not used in the ith round. However, all 64 bits of RK_i, as output from the encryption with K, are used as feed-forward value in the generation of the subsequent subkey.

The design principles of the key schedule are, first, the subkeys should depend on many master key bits, but without requiring too much work, second, on input s 64-bit (master)keys, any s consecutive subkeys should have an entropy of $56 \cdot s$ bits, and finally, there should be no obvious related and weak keys and the complementation property should not hold. Note that the latter two problems are present in the DES and all three are present in triple-DES. We note that if the master keys are of 64 bits each, it might be possible to find a pair of keys which generate the same set of subkeys. However, the number of such keys are expected to be so small that they pose no threat for DEAL when used for encryption.

The offsets $\langle i \rangle$ are introduced to avoid weak keys. If they are not present, there exist keys for which all subkeys are equal. E.g., for DEAL-128 the keys $K_1 = K_2 = D_K(0)$ would generate 6 subkeys all with value zero. Together with the offsets the encryptions with a fixed key avoid the existence of weak and related keys and the complementation property.

Note that the effective key lengths of the proposals are 112, 168, and 224 bits, respectively, if a parity bit is used in every byte of the master key.

There are several possible alternatives to the above structure of DEAL. Instead of the Feistel structure one could use the structure of MISTY, first described in [12], which allows for a higher degree of parallelism (in hardware). However, this structure is rather new and has not been extensively analysed. Another possibility is to use DEAL in "DES-X" mode [8], where an additional key is XORed to the plaintext and to the ciphertext. Alternatively, instead of using DES in the round function, one could use DES-X. The drawback of the latter two suggestions is that more subkeys would need to be generated and thus the key schedule of DEAL would become more complex.

2.1 Security of DEAL

What can we say about the security of DEAL in general? First note that for DEAL with 6 respectively 8 rounds a simple meet-in-the-middle attack (similar to the one on double-DES [6, 19]) will find the keys in the time of about 2^{168} respectively 2^{224} encryptions, independent of the key schedule. This is the reason that we suggest to do at least 8 rounds of encryption for DEAL-256. For DEAL-128 an exhaustive search for the key takes the time of about 2^{112} encryptions.

In [17] Patarin showed that to distinguish a 5 or 6-round n-bit Feistel cipher where the round function is a random function from a truly random $2n$-bit permutation, requires the knowledge of at least $2^{2n/3}$ plaintexts and their corresponding ciphertexts. He further conjectured that 2^n pairs are required. If we assume that the DES models a random permutation[1], Patarin's conjecture says that one needs about 2^{64} encryptions to distinguish DEAL from a random permutation, which is also the complexity of the matching ciphertext attack. The fastest known key-recovery attack on DEAL (with 6 rounds), that we are aware of, is the general attack on 6-round Feistel ciphers of [10], which applied to DEAL requires about 2^{121} DES-encryptions using about 2^{70} chosen plaintexts, which works for any key schedule. In the following a *difference* of two bit strings is defined as the bitwise XOR of the strings.

Proposition 1 *There is an attack on six-round DEAL with independent round keys, which requires about 2^{121} DES-encryptions using about 2^{70} chosen plaintexts.*

Proof: Consider a 5-round version and a pair of plaintexts with difference $\alpha \neq 0$ in the right halves and with equal left halves. Assume that the ciphertexts after 5 rounds have a difference of α in the left halves and are equal in the right halves. This necessarily means that the two inputs to the DES (in the round function of DEAL) are equal both in the first and the fifth rounds. Subsequently, the difference in the inputs to the DES in both the second and fourth rounds are α. But this necessarily means that the outputs of the DES in the third round are equal, which again means that the inputs to the DES in the third round are equal. This leads to a contradiction, since this means that the outputs of the DES in both the second and fourth round must be equal, which is not possible, since the inputs are assumed not to be equal. So the assumption that the ciphertexts after 5 rounds have differences α and zero in the left respectively right halves was wrong. In other words, we have defined a 5-round differential with probability zero. This can be used to attack DEAL.

The attack goes as follows. Choose 2^{64} plaintexts with a fixed left half and variable right half, say $P_i = (L, X_i)$ for $i = 1, \ldots, 2^{64}$. Let $C_i = (Z_i, W_i)$ denote the corresponding ciphertexts. Compute $X_i \oplus W_i$ and find matches $X_i \oplus W_i = X_j \oplus W_j$ for $i \neq j$. One can expect about 2^{63} such matches, since $\binom{2^{64}}{2} / 2^{64} \simeq 2^{63}$. Let $\alpha = X_i \oplus X_j = W_i \oplus W_j$.

[1]Note, that although the best known attack on the DES, the linear attack by Matsui [11], needs "only" 2^{43} known plaintexts, the attack requires that all these plaintexts and ciphertexts are known, which cannot be assumed for the applications of the DES in DEAL.

For all these matching pairs and for all values of the key in the sixth round decrypt the ciphertexts one round. If the differences in the ciphertext halves after 5 rounds are α and zero, the guessed value of the key is wrong. Note that for the correct value of the key in the sixth round one never obtains these differences after the fifth round, but for wrong values of the key this will happen with probability 2^{-64} for each analysed pair. Thus with 2^{63} pairs about half of the keys will have been discarded. By repeating the attack 56 times, only a few values of key in the sixth round will be left suggested. Totally the attack requires $56 \cdot 2^{64} \simeq 2^{70}$ chosen plaintexts, $(2^{56} + 2^{55} + 2^{54} + \ldots + 2 + 1) \cdot 2^{64} \simeq 2^{57} \cdot 2^{64} = 2^{121}$ DES-encryptions, and 2^{64} words of memory. □

The above attack applied to DEAL-192 is faster than an exhaustive search for the key, although the prerequisites are very unrealistic. If an attacker should succeed in getting 2^{64} or more pairs of plaintexts and ciphertexts, the matching ciphertext attack would come into play and a bigger block cipher is needed anyway. The best known attack on DEAL-128 is an exhaustive search for the key taking the time of about 2^{112} encryptions. We have found no attack on DEAL with 8 rounds better than the meet-in-the-middle exhaustive key search attack described above. There may be a faster attack, for example a clever extension of the above attack on 6 rounds, but such an attack will require unrealisticly many chosen plaintexts and an unrealistic amount of memory.

The attack on 6 rounds gives the explanation of our recommendation of $r \geq 6$ for DEAL. With $r \leq 5$ it is possible to specify differentials with probability zero. That is, for certain differences in a pair of plaintexts, other certain differences in the pair of ciphertexts are not possible. First of all, such a property is not present in any of the modern block ciphers, secondly, such differentials can be used in key-recovery attacks with complexity of about 2^{88} for DEAL with only 5 rounds [10]. (Note that this attack is only an upper bound of the security level).

We close this section by summing up the features of DEAL.

- DEAL has a 128-bit block size and allows for key sizes of 128, 192, and 256 bits (the effective key sizes are 112, 168, and 224 bits, respectively).
- The matching ciphertext attack requires about 2^{64} ciphertext blocks.
- No known, feasible attacks.
- DEAL with 6 rounds is as fast as triple-DES.
- DEAL can be used in the standard modes of operation.
- DEAL can be implemented using existing DES-hardware or DES-software.
- There are no obvious weak keys and the complementation property does not hold.

Let us finally note, that because of the rather complex key schedules, DEAL is probably not practical for use in hash functions.

3 Concluding Remarks

We described a block cipher, DEAL, with 128 bit blocks and 128-bit, 192-bit, and 256-bit keys, as an alternative to the existing triple encryption modes. DEAL can be used in all 4 standard modes developed for the DES. For the first two key sizes the scheme encrypts two 64-bit plaintexts using six DES encryptions, thus has a performance equal to triple-DES. DEAL with 8 rounds (with a key size of 256 bits) performs equally to the CBCM mode used with DES. Because of the large key and block sizes, exhaustive key search and the matching ciphertext attack are infeasible. In addition, the weaknesses of the DES and triple-DES are avoided. There are no obvious weak keys, the complementation property does not hold, and the related key attacks are very unlikely to succeed. We recommend that ANSI adopts DEAL as part of [21]. Also, we suggest DEAL as a possible candidate for the Advanced Encryption Standard [14].

4 Acknowledgments

The author is grateful to Don Coppersmith, Bart Preneel, Vincent Rijmen and Matthew Robshaw for many valuable comments.

References

[1] E. Biham. Cryptanalysis of multiple modes of operation. In J. Pieprzyk and R. Safavi-Naini, editors, *Advances in Cryptology - ASIACRYPT'94*, pages 278–292. Springer Verlag, 1995.

[2] E. Biham and L.R. Knudsen. Cryptanalysis of the ANSI X9.52 CBCM mode. In K. Nyberg, editor, *Advances in Cryptology - EuroCrypt'98*. Springer Verlag, 1998. To appear.

[3] M. Blaze, W. Diffie, R.L. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Wiener. Minimal key lengths for symmetric ciphers to provide adequate commercial security. Document, January 1996.

[4] D. Coppersmith, D.B. Johnson, and S.M. Matyas. A proposed mode for triple-DES encryption. *IBM Journal of Research and Development*, 40(2):253–261, March 1996.

[5] D. Coppersmith, D.B. Johnson, and S.M. Matyas. Triple DES cipher block chaining with output feedback masking. Technical Report RC 20591, IBM, October 1996. Presented at the rump session of CRYPTO'96.

[6] W. Diffie and M. Hellman. Exhaustive cryptanalysis of the NBS data encryption standard. *Computer*, pages 74–84, 1977.

[7] J. Kelsey, B. Schneier, and D. Wagner. Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and triple-DES. In Neal Koblitz, editor, *Advances in Cryptology: CRYPTO'96, LNCS 1109*, pages 237–251. Springer Verlag, 1996.

[8] J. Kilian and P. Rogaway. How to protect DES against exhaustive key search. In Neal Koblitz, editor, *Advances in Cryptology: CRYPTO'96, LNCS 1109*, pages 252–267. Springer Verlag, 1996.

[9] L.R. Knudsen. *Block Ciphers – Analysis, Design and Applications.* PhD thesis, Aarhus University, Denmark, 1994.

[10] L.R. Knudsen. On the security of Luby-Rackoff ciphers in practice. In preparation, 1998.

[11] M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology: EUROCRYPT'93, LNCS 765*, pages 386–397. Springer Verlag, 1993.

[12] M. Matsui. New structure of block ciphers with provable security against differential and linear cryptanalysis. In D. Gollman, editor, *Fast Software Encryption, Third International Workshop, Cambridge, UK, February 1996, LNCS 1039*, pages 205–218. Springer Verlag, 1996.

[13] U.M. Maurer. New approaches to the design of self-synchronizing stream ciphers. In D.W. Davies, editor, *Advances in Cryptology: EUROCRYPT'91, LNCS 547*, pages 458–471. Springer Verlag, 1991.

[14] NIST. AES announcement. Draft, June 15, 1997.

[15] National Bureau of Standards. Data encryption standard. Federal Information Processing Standard (FIPS), Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.

[16] National Bureau of Standards. DES modes of operation. Federal Information Processing Standard (FIPS), Publication 81, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., December 1980.

[17] J. Patarin. How to construct pseudorandom and super pseudorandom permutations from one single pseudorandom function. In R.A. Rueppel, editor, *Advances in Cryptology - EUROCRYPT'92, LNCS 658*, pages 256–266. Springer Verlag, 1993.

[18] W. Tuchman. Hellman presents no shortcut solutions to DES. *IEEE Spectrum*, 16(7):40–41, July 1979.

[19] P.C. van Oorschot and M.J. Wiener. Improving implementable meet-in-the-middle attacks of orders of magnitude. In Neal Koblitz, editor, *Advances in Cryptology: CRYPTO'96, LNCS 1109*, pages 229–236. Springer Verlag, 1996.

[20] M.J. Wiener. Efficient DES key search. Technical Report TR-244, School of Computer Science, Carleton University, Ottawa, Canada, May 1994. Presented at the Rump Session of CRYPTO'93.

[21] ANSI X9.F.1. TDEA modes of operation. Draft 5.5, X9.52, March 29, 1996.