J. Cryptology (1998) 11: 45–58

Journal of
CRYPTOLOGY

Cryptanalysis of Multiple Modes of Operation

Eli Biham
Computer Science Department, Technion—Israel institute of Technology,
Haifa 32000, Israel
biham@cs.technion.ac.il
WWW: http://www.cs.technion.ac.il/~biham/

Communicated by Don Coppersmith

Received 15 February 1996 and revised 30 May 1996

Abstract. In recent years, several new attacks on DES were introduced. These attacks have led researchers to suggest stronger replacements for DES, and in particular new modes of operation for DES. The most popular new modes are triple DES variants, which are claimed to be as secure as triple DES. To speed up hardware implementations of these modes, and to increase the avalanche, many suggestions apply several standard modes sequentially. In this paper we study these *multiple* (cascade) modes of operation. This study shows that many multiple modes are much weaker than multiple DES, and their strength is theoretically comparable to a single DES.

We conjecture that operation modes should be designed around an underlying cryptosystem without any attempt to use intermediate data as feedback, or to mix the feedback into an intermediate round. Thus, in particular, triple DES used in CBC mode is more secure than three single DESs used in triple CBC mode. Alternatively, if several encryptions are applied to each block, the best choice is to concatenate them to one long encryption, and build the mode of operation around it.

Key words. Block ciphers, Modes of operation, Multiple modes.

1. Introduction

The Data Encryption Standard [16] has several modes of operation [17] in which it can be used. These modes were devised to have a limited error propagation, to allow synchronization in data communications, to hide patterns in the plaintexts, and to protect against chosen plaintext attacks on the underlying cryptosystem and against dictionary attacks. In the Cipher Block Chaining (CBC) mode and the Cipher Feedback (CFB) mode, each ciphertext block depends on all the previous plaintext blocks, by using the previous ciphertext block during encryption. The Output Feedback (OFB) mode was designed to allow precomputation of a major part of the encryption process, and to act as a pseudorandom bit generator. In this mode, a chosen plaintext attack does not allow an attacker more information than a known plaintext attack. The CFB and OFB modes also allow encryption with a variety of blocksizes. Figure 1 describes these standards.

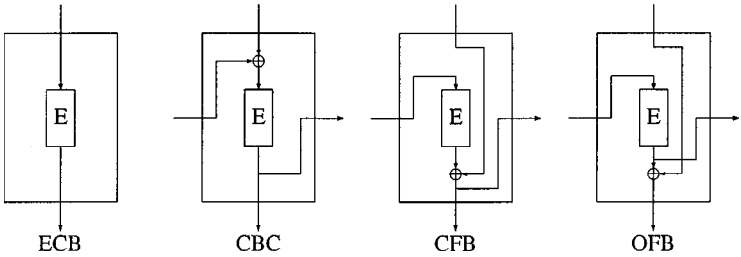

Fig. 1. DES modes of operation.

Although these modes were designed to protect against chosen plaintext attacks, there is no attempt to protect against known plaintext attacks. In the modes of operation of DES, if an attacker knows both the plaintext blocks and the ciphertext blocks, he can calculate the values of actual inputs and outputs of the underlying cryptosystem, and can mount any known plaintext attack.

Since the DES modes of operation were introduced, many new nonstandard modes were suggested. The first of which is the counter mode in which a counter is incremented and used as a feedback, while there is no feedback from other plaintext blocks. Other examples of suggested modes are PCBC, which was also used as a MAC function in the Kerberos system, and PFF (Plaintext Feed Forward) [10], which is similar to decryption under CBC (except that it uses encryption rather than decryption internally). All these modes are designed around one encryption function, without inner-feedbacks. We will call such modes *single modes*.

In recent years, several new attacks on DES were introduced: Differential cryptanalysis [4] requires 2^{47} chosen plaintexts and complexity in order to find the key, linear cryptanalysis [13] requires 2^{43} known plaintexts and complexity, and the improved Davies' attack [2] (see also [6] and [7]) requires 2^{50} known plaintexts. However, the main threat for the security of DES is exhaustive search for the keys on special purpose machines [8], [21], which can try keys so fast so that all the 2^{56} possible keys can be searched within only a few hours. These attacks have led many cryptographers to suggest stronger replacements to the DES, which can be either new cryptosystems or new modes of operation for the DES. The most popular new modes are the *multiple modes*, which are combined from several consecutive applications of single modes [10], [12]. In particular, *triple modes* combined from three consecutive applications of single modes were suggested. These triple modes were claimed to be as secure as triple DES, although they do not have triple DES as a building block. An advantage of the triple modes and multiple modes when implemented in hardware is that their speed is just the same as of single modes, since the single modes can be pipelined. Such triple-modes are candidates for ANSI standards.

We denote the modes by the notation $M_1|M_2|\cdots|M_n$, where the single mode M_1 is applied on the plaintext, the mode M_2 is applied on the output of M_1, and each mode M_i is applied on the output of the preceding mode M_{i-1}. The output of the multiple mode is the output of the last single mode M_n.

In this paper we cryptanalyze many multiple modes of operation and *find their keys*.

In particular, we show that many triple modes are much weaker than triple DES, and that some triple modes are not much more secure than a single DES.

Our attacks may be based upon any known attack on the underlying cryptosystems, and in particular differential cryptanalysis [4], linear cryptanalysis [13], improved Davies' attack [2], and exhaustive search. For reference we assume that the following complexities are required by these attacks: 2^{47} chosen plaintexts or 2^{55} known plaintexts are required for differential cryptanalysis of DES, and 2^{60} chosen plaintexts or 2^{61} known plaintexts if independent keys are used. 2^{43} known plaintexts are required for linear cryptanalysis of DES, and we estimate that 2^{60} known plaintexts are required if independent keys are used. Exhaustive search requires $2^{55} - 2^{56}$ steps. For Feal-8 [20], [15] the complexities are 1000, 1000, 2^{24} (see [1]), 2^{24}, and 2^{64}, respectively. Note that all the complexities of differential cryptanalysis hold for the ECB, CBC, and the CFB modes (under chosen plaintext or chosen ciphertext attacks), and that the linear cryptanalysis complexities hold for the ECB, CBC, CFB, and the OFB modes (under a known plaintext attack). (Note that an attack on the 8-bit CFB mode of DES with a reduced number of rounds was described in [19]). The best full-round differential characteristic of DES has probability about 2^{-62} and the best full-round differential characteristic of Feal-8 has probability 2^{-16}. Unless otherwise indicated, we assume that DES is the underlying cryptosystem of the attacked modes.

Our attacks are of three major kinds: Chosen plaintext attacks are applicable to the ECB mode and to many other modes. Chosen ciphertext attacks are applicable to many of the modes with limited error propagation. For example, the CBC and the CFB modes are vulnerable to chosen ciphertext attacks (with attacks much simpler than the ones described in this paper).

The third kind of attacks (which we do not actually apply in this paper) generalizes the chosen plaintext and chosen ciphertext attacks into chosen plaintext and ciphertext attacks, in which the attacker can decide for each block whether he chooses the plaintext or the ciphertext. These attacks are not adaptive: the attacker can choose all the plaintext/ciphertext blocks before he receives the first encrypted/decrypted block. This model is very strong, since in practice no encryption chip or software allows changing direction from encryption to decryption and vice versa during the process of encryption/decryption. We can slightly reduce this demand by viewing an equivalent model which does not require changing encryption/decryption direction for each block. In this model, two chips loaded with the same key are required: one of them always encrypts and the other always decrypts. In this model, the attacks are adaptive chosen plaintext on one chip and an adaptive chosen ciphertext on the other chip, both executed in parallel. Whenever in the original attacks we have to encrypt a block, we feed the encrypting chip with the plaintext block, and feed the decrypting chip with the resultant ciphertext. Whenever in the original attacks we have to decrypt a block, we feed the decrypting chip with the ciphertext block, and feed the encrypting chip with the resultant plaintext. This model is more realistic in the sense that each chip either encrypts or decrypts, but the adaptive attack requirement causes this attack to work almost only when two such loaded chips may be directly manipulated by the attacker. The chosen plaintext and ciphertext attacks can cryptanalyze many modes that cannot be attacked by the simpler attacks and can attack other modes with a smaller complexity than other attacks.

We show that many multiple modes are weaker than the corresponding multiple ECB mode, when chosen plaintext, chosen ciphertext, or chosen plaintext and ciphertext attacks are applicable. If a multiple mode combines several single modes, in which in each of them a different cryptosystem is used, and in which the keys of the various single modes are independent, the strength of the multiple mode is at least the strength of the strongest single mode component. If the various keys are not independent, the strength of the multiple mode might even be reduced to the strength of its weakest component. Two-key triple DES (triple ECB mode) is such an (already known) example [18].

Although in 3-key triple-DES we do not know how to find the key with less than 2^{112} steps, still given all the 2^{64} (known) plaintexts, we can store them in a table (dictionary), and encrypt/decrypt using the table, without even knowing the key. In other triple-modes that have intermediate feedbacks, such dictionary attacks are not applicable.

We conjecture that strong operation modes that are immune against finding their keys should be designed around an underlying cryptosystem without any attempt to use intermediate data as feedback, or to mix the feedback into an intermediate round. Alternatively, if several encryptions are applied in each block, the best choice is to concatenate them to one long encryption, and build the mode of operation around the result.

We emphasize that the results in this paper hold only to multiple modes of encryption. For example, the triple hash-function mode MD4|MD5|SHA is not collision-free, since MD4 is not collision-free [9].

This paper is divided into the following sections: In Section 2 we show that multiple modes are at least as strong as the strongest single mode contained within, when the keys of all the various single modes are independent. In Section 3 we analyze many multiple modes and describe our analysis techniques. In Section 4 we summarize the results.

2. The Strength of Multiple Modes

In this section we show that multiple modes of operation are not less secure than their strongest single mode component, whenever the keys of the various components are independent. This result holds in models in which the attacker has access to the plaintexts (and not only to their statistics). This result was already proved in the context of cascade ciphers in [11].[1]

Let A and B be two modes and let C be the combined double mode C = AB, whose component keys K_A and K_B are chosen independently. The following theorem shows that C is not weaker than either of its components. It is similar to Theorem 5 in [11], whose proof holds in our case as well.

Theorem 1. *The cracking problem of either A or B is efficiently reducible to the cracking problem of* C = AB.

[1] It does not hold when the attacker has access only to the statistics of the plaintexts [14]. In our model the attacker always knows both the plaintexts and the ciphertexts.

Conclusion 1. *A multiple mode may not be weaker than its strongest component, if the component keys are chosen independently.*

We show that this theorem holds *only* if the various components' keys are independent. In particular, it does not hold for two-key triple modes (such as encrypt with K_1, encrypt (or decrypt) with K_2, and encrypt with K_1 again), since it might be that one key (K_1) is used both in the strongest component and the weakest component, and then we might find it by attacking the weakest component. For example, we study the case of a triple CBC mode which uses Feal-8 [20], [15] in its first two components, and DES [16] in the third, while the same key K_1 is used in both the first component and the third component (see Fig. 2). By methods described in the next section, we can find the key K_1 of the first component using 2^{18} chosen ciphertexts. The key of the third component is the same as the key of the first component. The key of the second component can then be easily found using 1000 chosen ciphertexts (or 2^{24} known plaintexts). Therefore, the whole secret key of the multiple mode is found using about 2^{18} chosen ciphertexts within a few minutes. Note that the third component (which uses DES) by itself is much more resistant than the whole system, and cannot be attacked successfully by any known method with complexity smaller than 2^{43}.

3. Analysis

For the cryptanalysis of the modes of operation, we use several techniques. These techniques select one of the encryption boxes in the modes of operation, inside one of the single modes, and feed it with the data required for cryptanalysis by one of the known methods (differential, linear, improved Davies, or exhaustive search). After the key of

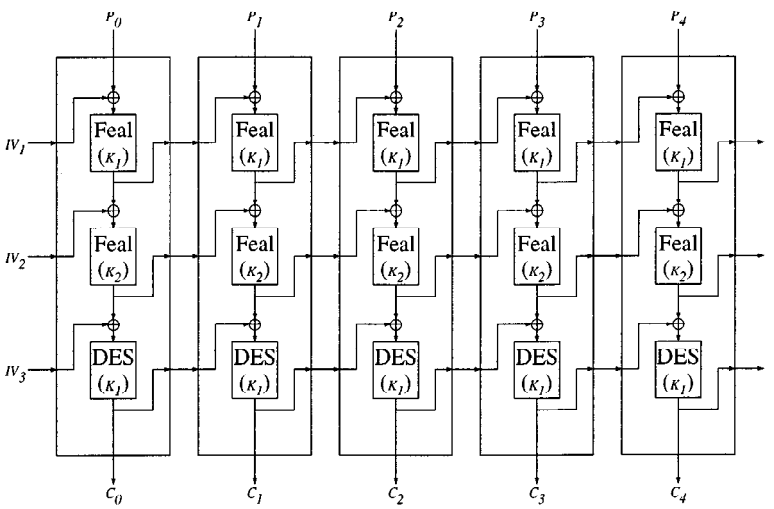

Fig. 2. The triple CBC mode, using Feal-8, Feal-8, and DES.

the encryption box is found, other (or the same) techniques are used to find the remaining keys (one at a time).

In the following sections we describe six cryptanalysis techniques, which introduce the most useful principles used to cryptanalyze multiple modes. Additional techniques can be developed using these principles. Each of the techniques finds one key. Unless otherwise indicated, the complexities quoted in the descriptions of these techniques are the complexities to find this one key. The total complexities of the attacks on the various modes are described in the summary. A few of the full attacks might become adaptive; however, in most cases the attacks remain nonadaptive.

We refer to the individual encryption operations used in the modes of operations as *encryption boxes* (whether they actually apply block encryption or block decryption), and number them with the index of the mode during the multiple encryption. In our discussion we use the terms *input* and *output* of the encryption boxes to be their input/output during mode encryption, and we keep the same terms even when we discuss decryption of the multiple mode. We keep the words *plaintext* and *ciphertext* to be the plaintext/ciphertext of the multiple mode, rather than to be the input/output of the encryption boxes. We also assume that the keys entering the encryption boxes are independent. We denote the key entering encryption box i by K_i, and the initial value of the ith single mode (if any) by IV_i (see Fig. 2).

3.1. *Technique A*: *A Technique Using Differential Cryptanalysis*

Our basic technique for analyzing multiple modes of operation is to feed one of the underlying encryption boxes (in one of the single modes) with the data required for differential cryptanalysis. This may be done by choosing pairs of tuples of blocks in such a way that most blocks are the same in both pairs, and these blocks cause many internal values to be fixed when both tuples are encrypted/decrypted. One block should differ by the difference required for differential cryptanalysis, and it should cause this difference to appear in the input (or output) of one of the encryption boxes. In addition, we should be able to collect the output (or input) of this encryption block, up to XOR with some of the fixed internal values. This situation allows us to attack the encryption box by the regular differential attacks to which it is vulnerable (if it is vulnerable). This technique can be based on any differential cryptanalytic attack, and any successful 0R-, 1R-, 2R-, or 3R-attack (i.e., attack which use characteristics shorter by 0, 1, 2, or 3 rounds than the cipher) can be applied.

One of the simplest forms of this technique attacks the ECB|CBC|CBC mode (see Fig. 3) using a chosen ciphertext attack. Our aim is to feed the output of encryption box 1 (in the single ECB component) with pairs differing by the differences required for differential cryptanalysis. After these pairs are decrypted, the inputs of the encryption box are just the plaintexts we receive from the decryption of the triple mode. Thus, the regular differential cryptanalytic techniques can be applied. Note that due to the symmetry of DES (and most blockciphers), there is no technical difference between a chosen plaintext and a chosen ciphertext attack on the blockcipher. Note also that if the value of two successive ciphertext blocks occurs twice in different positions in a ciphertext message (encrypted under the same keys with the ECB|CBC|CBC mode), the same feedbacks result in both positions, and any third block is decrypted into the same plaintext in both positions.

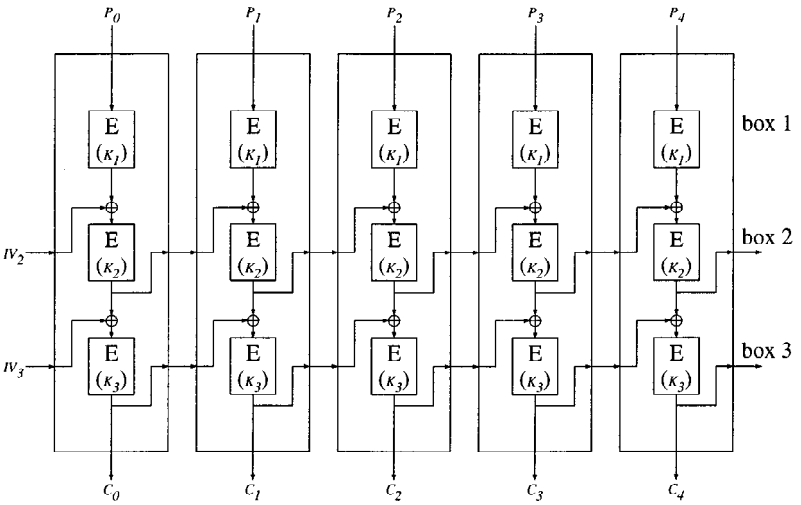

Fig. 3. The triple mode: ECB|CBC|CBC.

For the attack, the attacker chooses many pairs of tuples of blocks (C_0, C_1, C_2) and $(C_0 \oplus \Omega_T, C_1, C_2)$, where C_0, C_1, and C_2 are some arbitrary block values, and Ω_T is the difference required for differential cryptanalysis. If a differential attack with Ω_T requires n pairs to attack an ECB mode, the attacker should choose n tuples (C_0, C_1, C_2) and request to decrypt the $6n$ blocks consisting of all the pairs (C_0, C_1, C_2) and $(C_0 \oplus \Omega_T, C_1, C_2)$.

It is evident that the difference of the tuples is $(\Omega_T, 0, 0)$ for each pair. Due to the structure of the triple mode, the differences 0 cause differences 0 in the input of box 3, and after XORing these differences with the differences of the feedbacks, we result with differences $(-, \Omega_T, 0)$ in the output of box 2, where "$-$" denotes an unpredictable value. Similarly, the differences at the output of box 1 are $(-, -, \Omega_T)$. Therefore, in the third blocks of the tuples, the differences of the output of box 1 are Ω_T, just as chosen by the attacker. Since the input of box 1 is the plaintext received by decryption of the triple mode, all the requirements for differential cryptanalysis of box 1 are satisfied. As a result, we can find the key used in box 1 by applying differential cryptanalytic attacks.

The attack described above assumes that the characteristic is set in the last rounds of box 1, and that the analysis is done on the first rounds. This attack can use quartets, octets, or structures of any size by fixing C_1 and C_2 and playing with structures of C_0.

This technique, as described above, does not apply to the differential attack on the full 16-round DES [3], [4], since the latter requires the knowledge of actual plaintext (in our case: ciphertext) bits, and not only their differences. However, the 14 plaintext (ciphertext) bits required by the attack, are not known to the attacker just because they are XORed with a 14-bit constant. This constant can be found together with the key using a more extensive analysis, by doing the rest of the analysis for each of the 2^{14} possibilities, since the analysis complexity in the attack on the 16-round DES is only 2^{37}. Thus, the complexity of a differential cryptanalytic attack on the first key of this triple mode is about $2^{37} \cdot 2^{14}/3 \approx 2^{49}$ triple-DES encryptions, given about $3 \cdot 2^{47}$ chosen

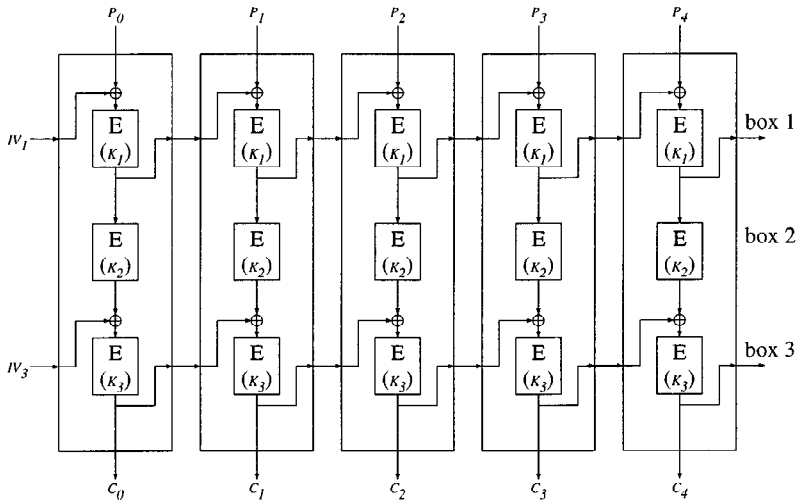

Fig. 4. The triple mode: CBC|ECB|CBC.

ciphertexts (2^{47} chosen ciphertext tuples). Using auxiliary structuring techniques, the number of chosen ciphertexts can be reduced to 2^{47}.

3.2. *Technique B*: *Enhancement of Technique A*

An enhancement of Technique A allows attacking modes whose plaintexts are mixed with feedbacks before they are fed into the first encryption box. Examples of such modes are CBC|ECB|CBC and CBC|CBC|ECB. These modes are described in Figs. 4 and 5. This enhanced technique may also use any 0R-, 1R-, 2R-, or 3R-attack, but requires finding more than one subkey. Thus, the number of required plaintexts is similar to the number of plaintexts required by the independent key variant of the differential cryptanalytic attack.

In these modes, we choose the differences of the tuples just as we do in Technique A, but we receive less information from the received plaintexts. In Technique A the inputs of encryption box 1 are known to the attacker. In the generalized modes attacked by this enhanced technique, we first attack the ECB mode, but the inputs of the encryption box in the ECB mode (boxes 2 and 3, respectively) are not known to the attacker. Thus, the chosen ciphertext tuples are of the form (C_0, C_1, C_2) and $(C_0 \oplus \Omega_T, C_1, C_2)$, where C_0 is chosen arbitrarily for each tuple, but C_1 and C_2 are fixed for all the tuples. As a result, the value of the input of the ECB mode equals the last plaintext block of the tuple XORed with an unknown fixed value (which depends only on C_1 and C_2, and is fixed in all tuples). For the analysis, this fixed value may be viewed as part of the (actual) subkeys of the ECB mode. The independent-key variant of the differential cryptanalytic attack can now find all the actual subkeys (only three actual subkeys are actually required for the attacks). By analyzing the actual subkeys, we can find two (complementary) possible values for the key and the fixed value. By trying the remainder of the analysis twice (for each of the two values), we can identify the complete key. The complexity of this attack

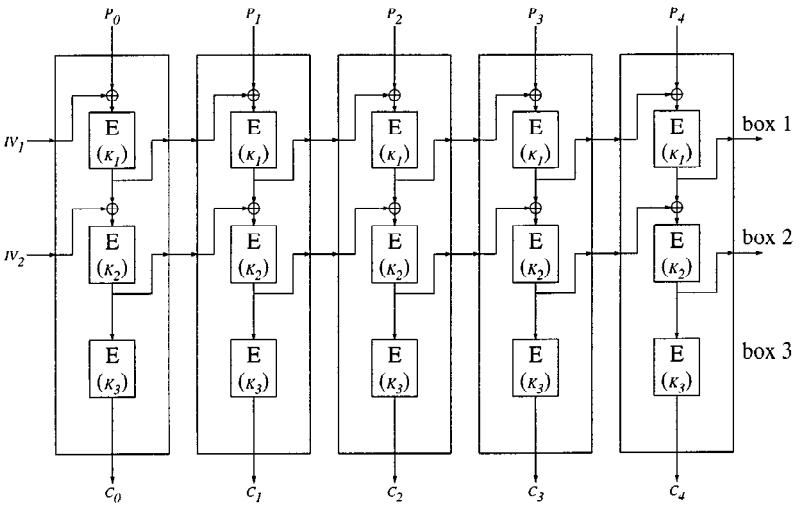

Fig. 5. The triple mode: CBC|CBC|ECB.

is similar to the complexity of the the independent key variant of the original attack on the ECB mode.

In the CBC|CBC|ECB mode, the other keys can be found by Technique D (as in the attack on the triple CBC mode described later). In the CBC|ECB|CBC mode, K_3 can be found easily, since the input of box 3 can be easily calculated; then, K_1 can also be completed.

3.3. *Technique C*: *A Technique Using Linear Cryptanalysis*

In this technique, we do not choose pairs of messages and study their differences, as we do when differential cryptanalysis is used. Instead, we fix many blocks which are mixed with the inputs/outputs of the attacked encryption box, and we end up with the knowledge of the inputs and the outputs of the attacked encryption box XORed with some unknown fixed values. Since linear cryptanalysis is not affected by the combination of such fixed values, we can do the whole linear cryptanalysis, just as is done in the regular model (i.e., single ECB mode)—we just end up with parity bits combining key bits and bits of the fixed values. Since linear cryptanalysis can also find the subkeys when independent keys are used (i.e., when all the subkeys are independent), we can complete the encryption keys even in this more complex case, after we find several subkeys, rather than just one or two.

This technique can be applied to the modes attacked by Techniques A and B. For example, to attack the CBC|ECB|CBC mode, it requires choosing many tuples of ciphertexts (C_0, C_1, C_2) where C_1 and C_2 should be fixed in all the tuples, and C_0 can be chosen at random. The resultant plaintext block P_2 is of the form $D_{K_2}(C_0 \oplus V_1) \oplus V_2$, where V_1 and V_2 are fixed values depending on the choice of the fixed ciphertext blocks C_1 and C_2. Linear cryptanalysis can find the key K_2 and the fixed values V_1 and V_2 (except one bit due to the complementation property: simultaneous complementation of

K_2, V_1, and V_2 does not change the results). Then, attacks to find K_1 and K_3 can be mounted (even exhaustive search for each of them requires now only $2^{55} - 2^{56}$ steps, and faster attacks are feasible).

This technique requires 2^{60} chosen tuples of ciphertext to find the key of the ECB component. The other keys of the CBC|ECB|CBC mode can be found even by exhaustive search with complexity about 2^{55}. The other keys of the ECB|CBC|CBC and the CBC|CBC|ECB modes should be found by Techniques D or F.

Similar techniques can use the known plaintext variant of differential cryptanalysis and the improved Davies' attack [2], but their complexities are expected to be higher than with linear cryptanalysis, when DES is the underlying cipher.

3.4. *Technique D*

In Technique B we used the single ECB component within the multiple mode to allow a fixed value to be XORed to the input pairs of the ECB component, and thus we could handle the additional mixing of the plaintexts before they are entered to the encryption boxes. Whenever we do not have a single ECB component in our mode, like in the triple CBC mode (CBC|CBC|CBC), we can use another enhancement of Technique A, that allows us to find the keys of the encryption boxes.

For the triple CBC mode, we choose the pairs of four-block tuples (C_0, C_1, C_2, C_3) and $(C_0, C_1 \oplus \Omega_T, C_2, C_3)$ (with the difference $(0, \Omega_T, 0, 0)$), with the same C_0, C_1, and C_2 in all the pairs. The various pairs differ only in the values of C_3, while the two members of a single pair differ only in the value of C_1. Thus, the differences are developed during decryption to $(-, A, \Omega_T, 0)$ at the output of encryption box 2, and to $(-, -, B, \Omega_T)$ at the output of encryption box 1, where A and B are some fixed differences in all the pairs (since they depend only on C_0, C_1, C_2, and Ω_T which are the same in all the pairs). As a result, encryption box 1 has difference Ω_T in the output of the fourth block, and its input difference is known to the attacker as the plaintext difference XORed with the unknown fixed value B. Once we find the value of B, Technique B can be used to find the key K_1.

The value of B can be found using a full-round characteristic of encryption box 1. If DES is used, it has probability about 2^{-62}, which (for many keys) will allow identifying the expected difference of the input to this box. Since the known plaintext block P_3 is XORed with the feedback from the previous block to form the input to the box, the differences satisfy $B = P_3' \oplus \Omega_P$, and B can be calculated for any right pair (P_3' is the difference between the plaintext block P_3 and its counterpart). The true value of B should be the most frequent resulting value, if the probability of the characteristic is not too low, and thus it can be identified (possibly using a huge memory of 2^{64} one-byte counters). This identification can be somewhat easier if we use the observation that we can find 52 bits of B even if we use only a 15-round characteristic, whose probability is about 2^{-55}, since we can predict the behavior of five S boxes in the sixteenth round (which have zero input differences).

This enhanced technique requires about 2^{65} chosen ciphertext tuples to find B, both feedbacks to P_3 (whose difference is B) and the key K_1. It requires full-length characteristics, whose number of rounds is the same as the number of rounds of the attacked encryption box (sometimes characteristics with one round less can be used), and thus

the number of required plaintexts is similar to the number of plaintexts required by a 0R-attack (1R-attack). This technique cannot use linear cryptanalysis.

One could also design modes with many feedbacks, that would seem more secure than modes with a small number of feedbacks. If we take this suggestion to the extreme, we could CBC-feedback every round of the triple-encryption, resulting with 48 feedbacks. This would make the intermediate data during the triple encryption be more dependent on the previous blocks, and would increase the avalanche. However, as we conclude from the triple CBC mode above, any multiple CBC mode is not more secure than its basic box against 0R-attacks. In this suggestion, the basic box is just one round, which is trivial to break. Thus, this extreme suggestion is also trivial to break. An attack requires only a few chosen ciphertexts to find all the subkeys, even if independent keys are used.

3.5. *Technique E*: *Using Exhaustive Search*

The best example of this technique analyzes the CBC|CBC|ECB mode. This technique finds the key of the last (ECB) encryption box using exhaustive search.

The attacker chooses one pair of ciphertext tuples (C_0, C_1, C_2) and (C_0^*, C_1, C_2) in which $C_0 \neq C_0^*$. For this pair, $P_2 \oplus P_2^*$ equals the difference of the input of the last encryption box of block 0. Thus, we can exhaustively search all values of K_3 by decrypting C_0 and C_0^* and verifying that the difference of the results equals $P_2 \oplus P_2^*$.

Unlike most of the techniques that we describe, this technique has a known plaintext variant. Given about 2^{65} known plaintexts, the birthday paradox predicts the existence of two tuples (C_0, C_1, C_2) and (C_0^*, C_1^*, C_2^*) in which $C_1 = C_1^*$, $C_2 = C_2^*$. The same technique might be applied on this pair.

3.6. *Technique F*: *The Birthday Technique*

This technique has several variants, of which only one is described in this section. All these variants use the birthday paradox to find good samples for cryptanalysis, and they can use differential cryptanalysis, linear cryptanalysis, and exhaustive search for finding the key of a single component. The variant we describe in this section cryptanalyzes the last encryption box of the triple CBC mode (or any multiple CBC/ECB mode whose last component is CBC), and it finds the key of the last component by exhaustive search.

This variant requires the attacker to choose 2^{33} ciphertext tuples of the form (C,C,C,C), where C is chosen at random, and to receive the corresponding plaintexts (P_0, P_1, P_2, P_3), of which only the P_3's are actually required.

The CBC decryption of the third single CBC mode of a tuple (C, C, C, C) results in $(?, H, H, H)$, where $H = C \oplus \mathrm{DES}_{k_3}^{-1}(C)$. H is a pseudorandom function of C (and not a permutation of the values of C). Thus, given 2^{33} random C's, with a high probability two of the C's result with the same H. Therefore, for these two C's, the same value of P_3 is expected. False alarms can result from the first two single CBC modes (due to the same property), and thus the following analysis should be repeated three times on average until K_3 is found.

Given the 2^{33} P_3's resulting from triple CBC decryption of the (C, C, C, C) tuples, we search for pairs of C and C^* for which $P_3 = P_3^*$. For such pairs we assume that both

C and C^* satisfy

$$C \oplus \mathrm{DES}_{k_3}^{-1}(C) = C^* \oplus \mathrm{DES}_{k_3}^{-1}(C^*).$$

Then, we exhaustively evaluate this equation for all the 2^{56} possible values of K_3. The equation is satisfied for a fraction of about 2^{-64} of the wrong keys, and thus we can be quite sure that a key satisfying this equation is the right key. (To decrease the false alarm probability further, we can select only keys which satisfy the equation using two different pairs of tuples). Note that after we find K_3, the same technique can find K_2 using the same data. Then, K_1 can be found by exhaustive search, differential cryptanalysis, or linear cryptanalysis.

A more sophisticated variant of this technique can attack the more complex CBC |CBC^{-1}|CBC (CBC encrypt, CBC decrypt, CBC encrypt) mode with 2^{66} chosen ciphertexts and complexity.

4. Summary

We studied the strength of multiple modes of operation. We showed that in many cases, these modes are weaker than the corresponding multiple ECB mode. In several cases, these modes are not more secure than just one single encryption using the same cryptosystem. For example, the triple CBC mode (CBC|CBC|CBC—whose components encrypt using a single DES) and the modes CBC|CBC|ECB, CBC|ECB|CBC, and ECB|CBC|CBC are weaker than triple DES, and their strength is comparable to the strength of a single DES. The triple mode CBC|CBC^{-1}|CBC, where CBC^{-1} is CBC decryption, is not much stronger.

Tables 1 and 2 summarize the results obtained for the multiple modes of operation when the underlying cryptosystems are DES and Feal-8, respectively. All the attacks are chosen ciphertext attacks. The complexities quoted are the complexities of finding one key of one of the single modes (i.e., the easiest key to find), in terms of the number of tuples required or the complexity of the analysis (the largest of them). To find the other keys the complexity might be higher. Table 3 summarizes the total complexities of attacking the multiple modes of operation, and finding all their keys.

We conclude that strong modes of operation, immune against finding their keys, should not be based on combining simpler modes, nor use internal feedbacks. We suggest using single modes, and incorporate multiple encryption as the underlying cryptosystems of the single modes. Alternatively, whenever we have a multiple mode or any other mode which uses internal feedbacks, it can be strengthened by eliminating the use of the internal feedbacks.

Acknowledgments

I would like to acknowledge Ross Anderson whose ideas motivated this research, to Carl Ellison and Burt Kaliski whose valuable remarks and suggestions improved the quality of this paper, to Don Coppersmith who found independently some of the results in this paper [5], to Shimon Even who pointed me to [11] and [14], and to Jennifer Seberry. I would also like to acknowledge the anonymous referee for his fruitful comments. This research was supported by the fund for the promotion of research at the Technion.

Table 1. Summary of the easiest-key (chosen ciphertext) attacks on multiple modes of DES.

	Cryptanalysis using technique					
Mode	A	B	C	D	E	F
ECB|CBC|CBC	2^{47}		2^{60}			2^{58}
CBC|ECB|CBC		2^{61}	2^{60}			2^{58}
CBC|CBC|ECB		2^{61}	2^{60}		2^{56}	
CBC|CBC|CBC				2^{66}		2^{58}
CBC|CBC^{-1}|CBC						2^{66}
CBC feedback every round				Few		

Table 2. Summary of the easiest-key (chosen ciphertext) attacks on multiple modes of Feal-8.

	Cryptanalysis using technique					
Mode	A	B	C	D	E	F
ECB|CBC|CBC	1000		2^{24}			2^{66}
CBC|ECB|CBC		1000	2^{24}			2^{66}
CBC|CBC|ECB		1000	2^{24}		2^{64}	
CBC|CBC|CBC				2^{17}		2^{66}
CBC|CBC^{-1}|CBC						2^{66}
CBC feedback every round				Few		

Table 3. Total complexities of the attacks on the multiple modes.

Mode	Complexity E = DES	Complexity E = Feal-8
ECB|CBC|CBC	2^{58}	2^{17}
CBC|ECB|CBC	2^{58}	2^{17}
CBC|CBC|ECB	2^{58}	2^{17}
CBC|CBC|CBC	2^{59}	2^{18}
CBC|CBC^{-1}|CBC	2^{66}	2^{66}
CBC feedback every round	Few	Few

References

[1] E. Biham, On Matsui's linear cryptanalysis, *Advances in Cryptology, Proceedings of EUROCRYPT* '94, pp. 341–355, Lecture Notes in Computer Science, Vol. 950, Springer-Verlag, Berlin, 1994.

[2] E. Biham and A. Biryukov, An improvement of Davies' attack on DES, *Advances in Cryptology, Proceedings of EUROCRYPT* '94, pp. 461–467, Lecture Notes in Computer Science, Vol. 950, Springer-Verlag, Berlin, 1994.

[3] E. Biham and A. Shamir, Differential cryptanalysis of the full 16-round DES, *Advances in Cryptology, Proceedings of CRYPTO* '92, pp. 487–496, Lecture Notes in Computer Science, Vol. 740, Springer-Verlag, Berlin, 1992.

[4] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, New York, 1993.

[5] D. Coppersmith, A chosen-ciphertext attack on one mode of triple DES CBC, Private communication, February 8, 1995.

[6] D. W. Davies, Investigation of a potential weakness in the DES algorithm, 1987, Private communication.

[7] D. Davies and S. Murphy, Pairs and triplets of DES S-boxes, *Journal of Cryptology*, Vol. 8, No. 1, pp. 1–25, 1995.

[8] W. Diffie and M. E. Hellman, Exhaustive cryptanalysis of the NBS data encryption standard, *Computer*, Vol. 10, No. 6, pp. 74–84, June 1977.

[9] H. Dobbertin, Cryptanalysis of MD4, *Proceedings of Fast Software Encryption, Cambridge*, pp. 53–69, Lecture Notes in Computer Science, Vol. 1039, Springer-Verlag, Berlin, 1996.

[10] C. Ellison, Private communication, 1993.

[11] S. Even and O. Goldreich, On the power of cascade ciphers, *ACM Transactions on Computer Systems*, Vol. 3, No. 2, pp. 108–116, May 1985.

[12] B. Kaliski, Triple-DES: A brief report, RSA Laboratories, Private communication, October 29, 1993.

[13] M. Matsui, Linear cryptanalysis method for DES cipher, *Advances in Cryptology, Proceedings of EUROCRYPT* '93, pp. 386–397, Lecture Notes in Computer Science, Vol. 765, Springer-Verlag, Berlin, 1993.

[14] U. M. Maurer and J. L. Massey, Cascade ciphers: The importance of being first, *Journal of Cryptology*, Vol. 6, No. 1, pp. 55–61, 1993.

[15] S. Miyaguchi, A. Shiraishi, and A. Shimizu, Fast data encryption algorithm FEAL-8, *Review of Electrical Communications Laboratories*, Vol. 36, No. 4, pp. 433–437, 1988.

[16] National Bureau of Standards, Data Encryption Standard, U.S. Department of Commerce, FIPS Publication 46, January 1977.

[17] National Bureau of Standards, DES Modes of Operation, U.S. Department of Commerce, FIPS Publication 81, December 1980.

[18] P. C. van Oorschot and M. J. Wiener, A known plaintext attack on two-key triple encryption, *Advances in Cryptology, Proceedings of EUROCRYPT* '90, pp. 318–325, Lecture Notes in Computer Science, Vol. 473, Springer-Verlag, Berlin, 1990.

[19] B. Preneel, M. Nuttin, V. Rijmen, and J. Buelens, Cryptanalysis of the CFB Mode of the DES with a reduced number of rounds, *Advances in Cryptology, Proceedings of CRYPTO* '93, pp. 212–223, Lecture Notes in Computer Science, Vol. 773, Springer-Verlag, Berlin, 1993.

[20] A. Shimizu and S. Miyaguchi, Fast data encryption algorithm FEAL, *Advances in Cryptology, Proceedings of EUROCRYPT* '87, pp. 267–278, Lecture Notes in Computer Science, Vol. 293, Springer-Verlag, Berlin, 1987.

[21] 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, August 1993.