On Modes of Operation

(Abstract)

February 22, 1994

Eli Biham
Computer Science Department
Technion - Israel Institute of Technology
Haifa 32000, Israel

Abstract

In this paper we study the modes of operation in which a cryptosystem, and in particular DES, can be used. This study shows that attempts to complicate the modes of operation weaken (in many cases) the resultant modes. We conclude that operation modes should be designed around the 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 a single-DES 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.

1 Introduction

The Data Encryption Standard[5] has several modes of operation[6] in which it can be used. The Electronic Code Book (ECB) mode encrypts each plaintext block independently of the other blocks. The Cipher Block Chaining (CBC) mode and the Cipher Feedback (CFB) mode were devised to have high dependence of the ciphertext blocks on all the previous plaintext blocks during encryption by feeding the previous ciphertext block into the encryption process of the next plaintext block, and the Output Feedback (OFB) mode was designed to allow precomputation of a major part of the encryption process, and to have no error extension. The CFB and OFB modes also allow encryption with a variety of blocksizes.

Since the DES modes of operation were introduced, many new non-standard 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. Another example of a suggested mode is PCBC, which was used as a MAC function in the Kerberos system.

One of the properties of the DES modes of operation and most other suggested modes is that under a known plaintext attack, the attacker can easily calculate the plaintext inputs and the ciphertext outputs of the internal cryptosystem from the plaintext blocks and the ciphertext blocks of the operation mode. Therefore, is was suggested[1] to devise operation modes which are not vulnerable to this weakness. In several of these modes, the feedback block is not known to the attacker, i.e., the feedbacks are partially encrypted ciphertexts under the same key or another key, or even an intermediate data from the internal encryption. In other such modes, the (possibly known feedback) is mixed into an intermediate round. When such modes are used, the system seems to resist better against

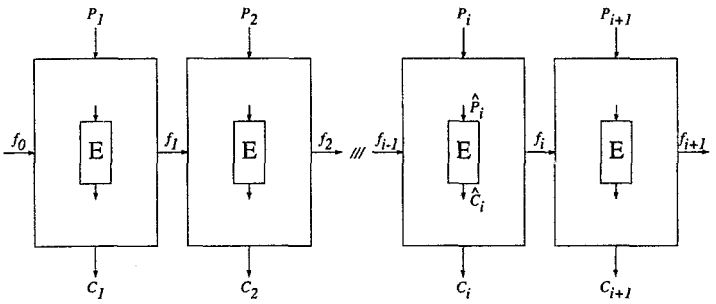

Figure 1. Outline of a Mode of Operation.

known plaintext attacks, since even exhaustive search becomes impossible. These modes are applicable only in software (or non-standard hardware), since the standard hardware does not allow to play with intermediate data.

Another application of such modes is when more than one encryption function is used for each block. For example, triple-DES may be used in CBC mode, where for each block three DES encryptions are applied. To increase the hardware speed (using pipelining), it is preferable to apply three levels of CBC mode, each use a single-DES[3].

We use the following notation. We denote the ith plaintext/ciphertext blocks (of the mode of operation) by P_i and C_i respectively. We assume that the blocksizes of P_i and C_i are the same as the blocksize of the underlying cryptosystem E. We denote the feedback block passed from the ith encryption to the $i+1$th encryption by f_i. Typically, the blocksize of f_i is the same as of P_i and C_i, but can be larger in particular modes. We also denote the plaintext input of the underlying cryptosystem by $\hat{P}_i$ and the ciphertext output by $\hat{C}_i$. Figure 1 describes this notation. An initial value f_0 (also called IV) is required by many modes. Each operation mode is characterized by the operations applied within each block in Figure 1. In Figure 2 the standard DES modes of operation are described.

Modes of operation can choose the feedback value f_i as any value calculated in the process, including f_{i-1}, P_i, $\hat{P}_i$, C_i, $\hat{C}_i$, any intermediate value during the encryption E of the underlying cryptosystem, an XOR-linear combination of these values, or any other function of these values. The feedback f_{i-1} can used by XORing it to any value in the process, including to P_i, $\hat{C}_i$, to an intermediate data during the encryption of $\hat{P}_i$ by E, or can be used as $\hat{P}_i$ itself. Another way to hide $\hat{P}_i$ is to encrypt the feedback by a second cryptosystem H before it is used.

In this paper we cryptanalyze modes of operation with a single feedback block. In order to compare the strength of the various modes of operation, we assume that the main factor of the strength of a cryptosystem against chosen plaintext attacks (and chosen ciphertext attacks) is the number of rounds. This assumption was shown to hold for many DES-like cryptosystems using differential cryptanalysis[2] and linear cryptanalysis[4].

We conclude that the feedback should not be chosen as an intermediate data of the underlying cryptosystem, neither be mixed with intermediate data. Such attempts will weaken the mode of operation against chosen plaintext attacks or chosen ciphertext attacks. We also conclude that if more than one application of a blockcipher is used to encrypt one plaintext block (for example, if the feedback is encrypted by H before used, or if triple-CBC is used), we can devise a new operation mode similar to the original mode, but in which the

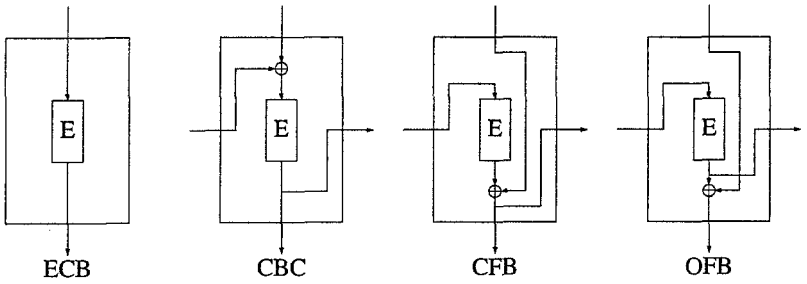

Figure 2. DES Modes of Operation.

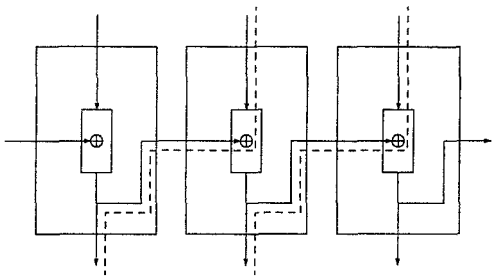

Figure 3. Shortest Path in a Mode of Operation.

various blockciphers are concatenated into a bigger blockcipher (e.g., CBC of triple-DES). This new mode uses the same underlying blockciphers as the original mode, and is more resistant to attacks.

2 Analysis

The DES modes of operation (except of the ECB mode) were designed to protect against chosen plaintext attacks on the underlying cryptosystem. In the CBC mode, the previous ciphertext block C_{i-1} should be known in order to be able to choose $\hat{P}_i$. In the CFB mode, an adaptive chosen plaintext attack should be used in order to choose $\hat{P}_i$. In the OFB mode, a chosen plaintext attack is just equivalent to a known plaintext attack. However, in all these modes 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 $\hat{P}_i$ and $\hat{C}_i$, and can mount a known plaintext attack against the underlying cryptosystem.

A proposal of Ross Anderson[1] is to protect against known plaintext attacks by modes whose feedbacks cannot be directly calculated from the plaintext or the ciphertexts, and thus either $\hat{P}_i$ or $\hat{C}_i$ (or both) are hidden from the attackers. He suggested to choose the feedback as the intermediate data after eight rounds of the internal DES. Other similar modes may encrypt the ciphertext by a reduced encryption H as a feedback, under the same key as of E, or under another key[1]. In these proposed modes, the attacker cannot identify $\hat{P}_i$, and cannot mount a known plaintext attack. Generalized forms of this idea can have feedbacks chosen as intermediate values during the internal encryption, and the

[1]in this example, if H is not keyed, it does not add any security to the system since the attacker can calculate it as well. In other examples, H can contribute to the strength even if it is not keyed, whenever the feedback is taken from an intermediate round.

feedback can be used (in the next block) by mixing it with an intermediate data during the internal encryption.

These suggestions are shown to reduce the security of the system. We show that the strength of an operation mode whose feedback contains only one wire against either chosen plaintext attacks or chosen ciphertext attacks is no more than the strength of the cryptosystem which is formed by the shortest path between a plaintext P_i and a ciphertext C_j through the (undirected) mode graph.

In this abstract we concentrate on one variant whose feedback is just the previous ciphertext block, and the feedback is XORed to the data after the eighth round, and we limit ourselves to an attack based on differential cryptanalysis. Figure 3 describes the shortest path of this mode. The shortest path contains only eight rounds of DES from C_i to P_{i+1}, and thus we claim that it is secure just as an eight-round DES. Nevertheless, an eight-round DES is already known to be much weaker than the full DES. The following chosen ciphertext attack can be mounted: Choose an encrypted message in a way such that for many i's:

$$C_{i+1} = C_{i+2} = C_i \oplus \Omega_P$$

where Ω_P is a value suggested by a characteristic as is required for the eight-round differential cryptanalytic attack on DES[2]. During decryption, the data in both blocks $i+1$ and $i+2$ are the same at rounds 9 to 16. After round eight the intermediate values are XORed with C_i and C_{i+1} which differ by Ω_P, and thus the data after the eighth round differ by Ω_P. During the next eight rounds of decryption (rounds eight to round one) the differences are predicted by the corresponding characteristic. Thus, the decrypted plaintext blocks P_{i+1} and P_{i+2} form pairs in the notation of differential cryptanalysis, in which the roles of encryption and decryption are reversed. The intermediate data differ after round eight by Ω_P, and P_{i+1} and P_{i+2} are known. Using many such pairs we can cryptanalyze this eight-round-path cryptosystem and find its key. In this particular case, about $3 \cdot 2^{15}$ chosen ciphertexts are required for the attack, since differential cryptanalysis requires 2^{15} pairs for the corresponding attack.

3 Summary

We studied the structure of modes of operation. We showed that if the feedback contains only one wire and at least one of its edges is connected to an intermediate-round data, the resulting mode becomes weaker than the underlying cryptosystem. Even if the feedback contains two or more wires, a similar property still holds in many cases. For example, a triple-CBC mode (doing CBC | CBC | CBC), each encrypts using a single-DES, is weaker than a single CBC mode of triple-DES (using a chosen ciphertext attack). The three modes CBC | CBC | ECB, CBC | ECB | CBC and ECB | CBC | CBC are even weaker than the triple-CBC mode, and their strength is just the same as of a single DES. Thus, we conclude that strong modes of operation (with simple feedback schemes) should feedback only external data to the underlying cryptosystem in order to preserve its strength, although this structure allows a known plaintext attacker to predict the exact plaintexts and ciphertexts encrypted by the underlying cryptosystem. Alternatively, whenever we have a mode which uses internal feedbacks, it can be strengthened by eliminating the use of the internal feedbacks, without affecting the underlying cryptosystems.

4 Acknowledgments

I would like to acknowledge Ross Anderson whose ideas motivated this research. Acknowledgment: This research was supported by the fund for the promotion of research at the Technion.

References

[1] Ross Anderson, private communications, 1993.

[2] Eli Biham, Adi Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.

[3] Carl Ellison, private communications, 1993.

[4] M. Matsui, *Linear Cryptanalysis Method for DES Cipher*, Abstracts of EUROCRYPT'93, pp. W112–W123, May 1993.

[5] National Bureau of Standards, *Data Encryption Standard*, U.S. Department of Commerce, FIPS pub. 46, January 1977.

[6] National Bureau of Standards, *DES Modes of Operation*, U.S. Department of Commerce, FIPS pub. 81, December 1980.