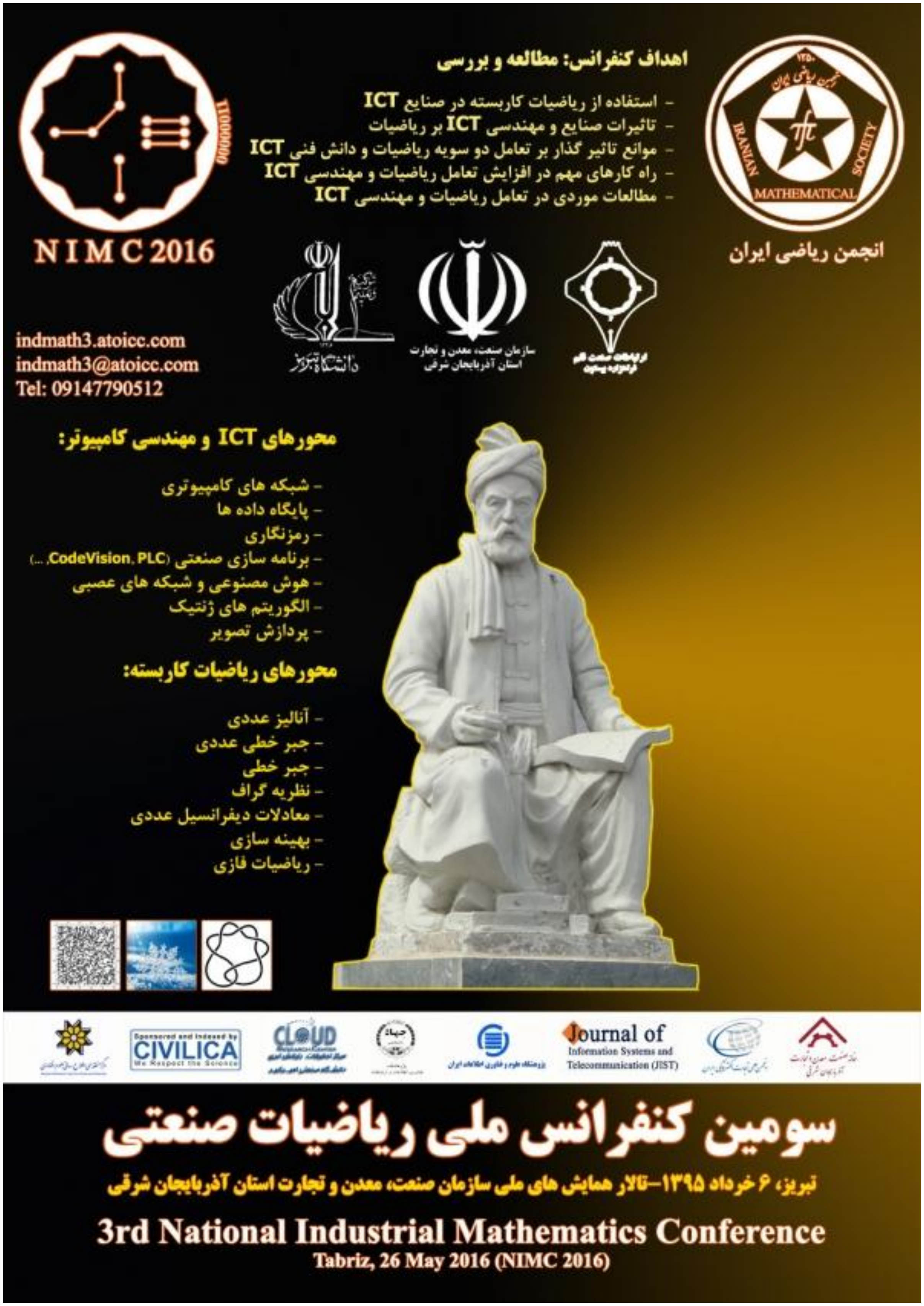
# Cryptanalytic attacks on DES block cipher



Mira Nasiri
University of Science and Culture



اهداف کنفرانس: مطالعه و بررسی
- استفاده از ریاضیات کاربسته در صنایع ICT
- تاثیرات صنایع و مهندسی ICT بر ریاضیات
- موانع تاثیر گذار بر تعامل دو سویه ریاضیات و دانش فنی ICT
- راه کارهای مهم در افزایش تعامل ریاضیات و مهندسی ICT
- مطالعات موردی در تعامل ریاضیات و مهندسی ICT
NIMC2016
انجمن ریاضی ایران
IRANIAN MATHEMATICAL SOCIETY
دانشگاه تبریز
سازمان صنعت، معدن و تجارت استان آذربایجان شرقی
indmath3.atoicc.com
indmath3@atoicc.com
Tel: 09147790512
محورهای ICT و مهندسی کامپیوتر:
- شبکه های کامپیوتری
- پایگاه داده ها
- رمزنگاری
- برنامه سازی صنعتی (CodeVision, PLC, ...)
- هوش مصنوعی و شبکه های عصبی
- الگوریتم های ژنتیک
- پردازش تصویر
محورهای ریاضیات کاربسته:
- آنالیز عددی
- جبر خطی عددی
- جبر خطی
- نظریه گراف
- معادلات دیفرانسیل عددی
- بهینه سازی
- ریاضیات فازی
Sponsored and Indexed by CIVILICA We Respect the Science
Journal of Information Systems and Telecommunication (JIST)
سومین کنفرانس ملی ریاضیات صنعتی
تبریز، ۶ خرداد ۱۳۹۵–تالار همایش های ملی سازمان صنعت، معدن و تجارت استان آذربایجان شرقی
3rd National Industrial Mathematics Conference
Tabriz, 26 May 2016 (NIMC 2016)

# Cryptanalytic attacks on DES block cipher

**Mira Nasiri**
mrnasiri@ee.sharif.edu
University of Science and Culture , Tehran, Iran

**Abstract:** This paper contains some of the cryptanalytic attacks. It covers several attack scenarios against ciphers known in literature. It deals with the method of cryptanalysis of block ciphers. Then, we will explain the specific attacks on DES block cipher in more details.

**Key Words**: Cryptanalytic attacks, DES block cipher, Cryptanalysis.

## Introduction

We give an overview of the various cryptanalytic attack scenarios that require minimal assumptions on the power and knowledge of the attacker to the most hypothetic attacks. Note that a long tradition in cryptanalytic research is that the attacker has full knowledge of the encryption algorithm, and only the key of the cryptosystem is unknown. This assumption is called a *Kerckhoff's* principle. There are many cryptosystems that are not broken under this condition, so why use one that is claimed to be secure, but is kept secret. This gives a false sense of security and in many cases tries to hide the lack of designer's expertise.

The aim of the attacker is to read the encrypted messages, which in many cases is achieved by finding the secret key of the system. The efficiency of the attack is measured by the amount of plaintext-ciphertext pairs required, time spent for their analysis and the success probability of the attack. Usually the starting point of a cryptanalytic attack is the ability, to distinguish the output of a cipher from the output of a random permutation.

**Chosen key attacks** This scenario is relevant in cases where Kerckhoffs' principle is violated, for example if components of a cipher such as S-Boxes are kept secret [14]. The attacker has full access to an encryption and/or decryption oracle that he can key. Chosen key attacks need not be adaptive chosen text attacks but can be combined with them.

**Related Key attacks** Related-Key attack is any form of cryptanalysis which the attacker can observe the operation of a cipher under several different keys whose values are initially unknown, but where some mathematical relationship connecting the keys is known to the attacker. For example, the attacker might know that the last 80 bits of the keys are always the same, even though he doesn't know, at first, what the bits are. This attack may discover interesting theoretical weaknesses in the key scheduling algorithm of a cipher.

In cases where Kerckhoff's principle does not apply, it can also be considered valid for an attacker to use chosen-key, chosen-text attacks to discover the inner structure of a block cipher. The first chosen-key attack in the literature is against the GOST 28147-89 block cipher [4], It is developed in the 1970s with secret S-Boxes. For this cipher Markku-Juhani Saarinen proposed a chosen-key attack that recovers the S-Boxes [13]. Some of the other ciphers prevent chosen-key scenarios by requiring the key to be provided together with a 160-bit checksum [11].

The models we have discussed thus far treat the cipher as an mathematically idealized building block with fixed inputs and outputs. In practice however, Eve is able to observe or even control more aspects of the execution of the actual ciphering algorithm. This gives rise to so-called side-channel attacks [14] and fault attacks [2].

## 1. Methods of cryptanalysis

In recent years, the exhaustive search attacks are obviously the most straightforward methods of cryptanalysis. In general, people expect that a good cipher is one for which the best attack is an exhaustive search for the key. The exhaustive search checks all the possible secret keys against a known plaintext/ciphertext sample. The correct key will produce the correct ciphertext from a known plaintext. The key-size of modern ciphers is picked large enough in order to make this method of attack impossible (128 bits or more). One of the major weaknesses of the DES cipher described further in this paper was its short key size (56 bits) which allows an exhaustive search attack[3].

## 2. About the attacks on DES block cipher

**Differential Cryptanalysis**. By encrypting a pair of carefully selected plaintexts under the same key to ciphertexts, the attacker is able to predict whether certain bits of the input to the last round are equal or not. This is achieved by using a difference pattern on the input. We describe this cryptanalysis in more details here on the DES cipher.

Differential cryptanalysis of DES [1] was the first method capable of breaking DES faster than exhaustive search. It is a statistical attack [12] which requires $2^{47}$ chosen plaintexts to break the DES cipher. It is based on the linearity of most of the operations used in DES;

$$
\begin{aligned}
E(X) \oplus E(X^{*}) &= E(X \oplus X^{*}) \\
(X \oplus K) \oplus (X^{*} \oplus K) &= X \oplus X^{*} \\
P(X) \oplus P(X^{*}) &= P(X \oplus X^{*})
\end{aligned} \tag{1}
$$

where E is the expansion operation, P is the permutation, and K is any subkey. The only nonlinear operations are the S-boxes, for which the equation

$$S(X) \oplus S(X^{*}) = S(X \oplus X^{*}) \tag{2}$$

does not hold. However, it was observed that for any particular input XOR not all the output XOR values are possible, and the possible ones do not appear uniformly, some of them appear more frequently then others. Using this observation the difference distribution table of an S-box can be defined as follows:

**Definition 1**. A table that shows the distribution of the input XORs and output XORs of all the possible pairs of an S-box is called the difference distribution table of the S-box[1].

In this table each row corresponds to a particular input XOR and each column corresponds to a particular output XOR. The entries themselves count the number of pairs out of 64 possible pairs with the particular input XOR that yield the particular output XOR.

Table 1. Partial XOR distribution table of $S_1$

| Input XOR | Output XOR | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $0_x$ | $1_x$ | $2_x$ | $3_x$ | $4_x$ | $5_x$ | $6_x$ | $7_x$ | $8_x$ | $9_x$ | $A_x$ | $B_x$ | $C_x$ | $D_x$ | $E_x$ | $F_x$ |
| $0_x$ | 64 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $1_x$ | 0 | 0 | 0 | 6 | 0 | 2 | 4 | 4 | 0 | 10 | 12 | 4 | 10 | 6 | 2 | 4 |
| $2_x$ | 0 | 0 | 0 | 8 | 0 | 4 | 4 | 4 | 0 | 6 | 8 | 6 | 12 | 6 | 4 | 2 |
| $3_x$ | 14 | 4 | 2 | 2 | 10 | 6 | 4 | 2 | 6 | 4 | 4 | 0 | 2 | 2 | 2 | 0 |
| $4_x$ | 0 | 0 | 0 | 6 | 0 | 10 | 10 | 6 | 0 | 4 | 6 | 4 | 2 | 8 | 6 | 2 |
| $5_x$ | 4 | 8 | 6 | 2 | 2 | 4 | 4 | 2 | 0 | 4 | 4 | 0 | 12 | 2 | 4 | 6 |
| $6_x$ | 0 | 4 | 2 | 4 | 8 | 2 | 6 | 2 | 8 | 4 | 4 | 2 | 4 | 2 | 0 | 12 |
| $7_x$ | 2 | 4 | 10 | 4 | 0 | 4 | 8 | 4 | 2 | 4 | 8 | 2 | 2 | 2 | 4 | 4 |
| $8_x$ | 0 | 0 | 0 | 12 | 0 | 8 | 8 | 4 | 0 | 6 | 2 | 8 | 8 | 2 | 2 | 4 |
| $9_x$ | 10 | 2 | 4 | 0 | 2 | 4 | 6 | 0 | 2 | 2 | 8 | 0 | 10 | 0 | 2 | 12 |
| $A_x$ | 0 | 8 | 6 | 2 | 2 | 8 | 6 | 0 | 6 | 4 | 6 | 0 | 4 | 0 | 2 | 10 |
| $B_x$ | 2 | 4 | 0 | 10 | 2 | 2 | 4 | 0 | 2 | 6 | 2 | 6 | 6 | 4 | 2 | 12 |
| $C_x$ | 0 | 0 | 0 | 8 | 0 | 6 | 6 | 0 | 0 | 6 | 6 | 4 | 6 | 6 | 14 | 2 |
| $D_x$ | 6 | 6 | 4 | 8 | 4 | 8 | 2 | 6 | 0 | 6 | 4 | 6 | 0 | 2 | 0 | 2 |
| $E_x$ | 0 | 4 | 8 | 8 | 6 | 6 | 4 | 0 | 6 | 6 | 4 | 0 | 0 | 4 | 0 | 8 |
| $F_x$ | 2 | 0 | 2 | 4 | 4 | 6 | 4 | 2 | 4 | 8 | 2 | 2 | 2 | 6 | 8 | 8 |
| $10_x$ | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 14 | 0 | 6 | 6 | 12 | 4 | 6 | 8 | 6 |
| $11_x$ | 6 | 8 | 2 | 4 | 6 | 4 | 8 | 6 | 4 | 0 | 6 | 6 | 0 | 4 | 0 | 0 |
| $12_x$ | 0 | 8 | 4 | 2 | 6 | 6 | 4 | 6 | 6 | 4 | 2 | 6 | 6 | 0 | 4 | 0 |
| $13_x$ | 2 | 4 | 4 | 6 | 2 | 0 | 4 | 6 | 2 | 0 | 6 | 8 | 4 | 6 | 4 | 6 |
| $14_x$ | 0 | 8 | 8 | 0 | 10 | 0 | 4 | 2 | 8 | 2 | 2 | 4 | 4 | 8 | 4 | 0 |
| $15_x$ | 0 | 4 | 6 | 4 | 2 | 2 | 4 | 10 | 6 | 2 | 0 | 10 | 0 | 4 | 6 | 4 |
| $16_x$ | 0 | 8 | 10 | 8 | 0 | 2 | 2 | 6 | 10 | 2 | 0 | 2 | 0 | 6 | 2 | 6 |
| $17_x$ | 4 | 4 | 6 | 0 | 10 | 6 | 0 | 2 | 4 | 4 | 4 | 6 | 6 | 6 | 2 | 0 |
| $18_x$ | 0 | 6 | 6 | 0 | 8 | 4 | 2 | 2 | 2 | 4 | 6 | 8 | 6 | 6 | 2 | 2 |
| $19_x$ | 2 | 6 | 2 | 4 | 0 | 8 | 4 | 6 | 10 | 4 | 0 | 4 | 2 | 8 | 4 | 0 |
| $1A_x$ | 0 | 6 | 4 | 0 | 4 | 6 | 6 | 6 | 6 | 2 | 2 | 0 | 4 | 4 | 6 | 8 |
| $1B_x$ | 4 | 4 | 2 | 4 | 10 | 6 | 6 | 4 | 6 | 2 | 2 | 4 | 2 | 2 | 4 | 2 |
| $1C_x$ | 0 | 10 | 10 | 6 | 6 | 0 | 0 | 12 | 6 | 4 | 0 | 0 | 2 | 4 | 4 | 0 |
| $1D_x$ | 4 | 2 | 4 | 0 | 8 | 0 | 0 | 2 | 10 | 0 | 2 | 6 | 6 | 6 | 14 | 0 |
| $1E_x$ | 0 | 2 | 6 | 0 | 14 | 2 | 0 | 0 | 6 | 4 | 10 | 8 | 2 | 2 | 6 | 2 |
| $1F_x$ | 2 | 4 | 10 | 6 | 2 | 2 | 2 | 8 | 6 | 8 | 0 | 0 | 0 | 4 | 6 | 4 |
| $20_x$ | 0 | 0 | 0 | 10 | 0 | 12 | 8 | 2 | 0 | 6 | 4 | 4 | 4 | 2 | 0 | 12 |
| $21_x$ | 0 | 4 | 2 | 4 | 4 | 8 | 10 | 0 | 4 | 4 | 10 | 0 | 4 | 0 | 2 | 8 |
| $22_x$ | 10 | 4 | 6 | 2 | 2 | 8 | 2 | 2 | 2 | 2 | 6 | 0 | 4 | 0 | 4 | 10 |
| $23_x$ | 0 | 4 | 4 | 8 | 0 | 2 | 6 | 0 | 6 | 6 | 2 | 10 | 2 | 4 | 0 | 10 |
| $24_x$ | 12 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 14 | 14 | 2 | 0 | 2 | 6 | 2 | 4 |
| $25_x$ | 6 | 4 | 4 | 12 | 4 | 4 | 4 | 10 | 2 | 2 | 2 | 0 | 4 | 2 | 2 | 2 |
| $26_x$ | 0 | 0 | 4 | 10 | 10 | 10 | 2 | 4 | 0 | 4 | 6 | 4 | 4 | 4 | 2 | 0 |
| $27_x$ | 10 | 4 | 2 | 0 | 2 | 4 | 2 | 0 | 4 | 8 | 0 | 4 | 8 | 8 | 4 | 4 |
| $28_x$ | 12 | 2 | 2 | 8 | 2 | 6 | 12 | 0 | 0 | 2 | 6 | 0 | 4 | 0 | 6 | 2 |
| $29_x$ | 4 | 2 | 2 | 10 | 0 | 2 | 4 | 0 | 0 | 14 | 10 | 2 | 4 | 6 | 0 | 4 |
| $2A_x$ | 4 | 2 | 4 | 6 | 0 | 2 | 8 | 2 | 2 | 14 | 2 | 6 | 2 | 6 | 2 | 2 |
| $2B_x$ | 12 | 2 | 2 | 2 | 4 | 6 | 6 | 2 | 0 | 2 | 6 | 2 | 6 | 0 | 8 | 4 |
| $2C_x$ | 4 | 2 | 2 | 4 | 0 | 2 | 10 | 4 | 2 | 2 | 4 | 8 | 8 | 4 | 2 | 6 |
| $2D_x$ | 6 | 2 | 6 | 2 | 8 | 4 | 4 | 4 | 2 | 4 | 6 | 0 | 8 | 2 | 0 | 6 |
| $2E_x$ | 6 | 6 | 2 | 2 | 0 | 2 | 4 | 6 | 4 | 0 | 6 | 2 | 12 | 2 | 6 | 4 |
| $2F_x$ | 2 | 2 | 2 | 2 | 2 | 6 | 8 | 8 | 2 | 4 | 4 | 6 | 8 | 2 | 4 | 2 |
| $30_x$ | 0 | 4 | 6 | 0 | 12 | 6 | 2 | 2 | 8 | 2 | 4 | 4 | 6 | 2 | 2 | 4 |
| $31_x$ | 4 | 8 | 2 | 10 | 2 | 2 | 2 | 2 | 6 | 0 | 0 | 2 | 2 | 4 | 10 | 8 |
| $32_x$ | 4 | 2 | 6 | 4 | 4 | 2 | 2 | 4 | 6 | 6 | 4 | 8 | 2 | 2 | 8 | 0 |
| $33_x$ | 4 | 4 | 6 | 2 | 10 | 8 | 4 | 2 | 4 | 0 | 2 | 2 | 4 | 6 | 2 | 4 |
| $34_x$ | 0 | 8 | 16 | 6 | 2 | 0 | 0 | 12 | 6 | 0 | 0 | 0 | 0 | 8 | 0 | 6 |
| $35_x$ | 2 | 2 | 4 | 0 | 8 | 0 | 0 | 0 | 14 | 4 | 6 | 8 | 0 | 2 | 14 | 0 |
| $36_x$ | 2 | 6 | 2 | 2 | 8 | 0 | 2 | 2 | 4 | 2 | 6 | 8 | 6 | 4 | 10 | 0 |
| $37_x$ | 2 | 2 | 12 | 4 | 2 | 4 | 4 | 10 | 4 | 4 | 2 | 6 | 0 | 2 | 2 | 4 |
| $38_x$ | 0 | 6 | 2 | 2 | 2 | 0 | 2 | 2 | 4 | 6 | 4 | 4 | 4 | 6 | 10 | 10 |
| $39_x$ | 6 | 2 | 2 | 4 | 12 | 6 | 4 | 8 | 4 | 0 | 2 | 4 | 2 | 4 | 4 | 0 |
| $3A_x$ | 6 | 4 | 6 | 4 | 6 | 8 | 0 | 6 | 2 | 2 | 6 | 2 | 2 | 6 | 4 | 0 |
| $3B_x$ | 2 | 6 | 4 | 0 | 0 | 2 | 4 | 6 | 4 | 6 | 8 | 6 | 4 | 4 | 6 | 2 |
| $3C_x$ | 0 | 10 | 4 | 0 | 12 | 0 | 4 | 2 | 6 | 0 | 4 | 12 | 4 | 4 | 2 | 0 |
| $3D_x$ | 0 | 8 | 6 | 2 | 2 | 6 | 0 | 8 | 4 | 4 | 0 | 4 | 0 | 12 | 4 | 4 |
| $3E_x$ | 4 | 8 | 2 | 2 | 2 | 4 | 4 | 14 | 4 | 2 | 0 | 2 | 0 | 8 | 4 | 4 |
| $3F_x$ | 4 | 8 | 4 | 2 | 4 | 0 | 2 | 4 | 4 | 2 | 4 | 8 | 8 | 6 | 2 | 2 |

Each line in a difference distribution table contains 64 pairs distributed over 16 entries[3]. Thus an average of the entries in each line of the table is exactly four. See the difference distribution table of $S_1$ of DES (Table 1). Note that the first line of the table shows that for the zero input XOR the output XOR must be zero. Also different lines in the table have different distributions and tables for different S-boxes are of course different. For example for $X \oplus X^* = 34_x$, $S_1(X) \oplus S_1(X^*) = 2_x$ for 16 pairs out of 64. In other words the input XOR difference $34_x$ causes the output XOR difference to be 2 with probability $p = 16/64 = 1/4$. Using the linearity of the rest of the operations in the cipher we receive probabilistic approximation of the difference of output of the F-function and thus one-round of DES. These approximations are called one-round characteristics[10]. It is possible to concatenate one-round characteristics in order to get longer characteristics. Here is a more strict definition of an n-round characteristic:

**Definition 2.** Associated with any pair of encryptions are the XOR value of its two plaintexts (denoted by $\Omega_P$), the XOR of its ciphertexts (denoted by $\Omega_C$) and the XORs of the inputs and of the outputs of each round in the two executions. These values form an n-round characteristic (denoted by $\Omega$). For a given input XOR $\Omega_P$, the probability that a randomly chosen input pair with $\Omega_P$ difference leads to $\Omega$ is called the probability of $\Omega$. It can be expressed as $P(\Omega|\Omega_P)$ [1].

We assume that in the process of concatenation of characteristics the probabilities of the characteristics are multiplied. This assumption can be justified empirically. It is important to note that there exist characteristics that can be concatenated with themselves. These characteristics are called iterative characteristics. We search for characteristics which have the highest probabilities. The higher is the probability of the characteristic that covers the whole cipher the less is the number of chosen plaintexts required for the attack. A useful notion of an active S-box may be introduced here.

**Definition 3.** An S-box $S_i$ is said to be active [1] in round *j* with respect to differential characteristic $\Omega$ if it has non-zero input difference in round j of $\Omega$.

The less is the number of active S-boxes in the differential characteristic $\Omega$ the higher is its probability. It can be shown that for DES the best characteristic can be built by iterating eight times a particular two-round characteristic [10]. See Figure1 for one such characteristic. The first round of this characteristic has $\psi \to 0$ _ XOR difference $\psi$ on the input of the F-function causes the output XOR difference of the F-function to be zero (with some probability). The second round of this characteristic has the form $0 \to 0$ which holds with probability one. In DES such a characteristic takes place for the difference $\psi = 19600000_x$. It involves three adjacent active S-boxes $S_1$, $S_2$, $S_3$ with input differences of $3_x = 000011_b$ , $32_x = 110010_b$ , $2C_x = 101100_b$ respectively (after $\psi$ has been expanded). The probability of this characteristic is:

$\frac{14.8.10}{64^3} \approx \frac{1}{234}$ which is rather low. This is due to the precautions taken by the designers of DES. They claim that they were aware of the high potential of differential cryptanalytic attacks.

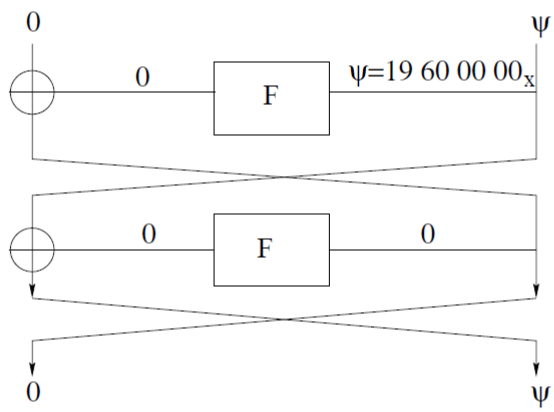



Figure 1. Two-round iterative characteristic of DES

**The Attack** Given the ideas described above, how the actual attack may work? In the simplest form, given a characteristic of probability $p >> 2^{-64}$ of the full cipher, it is possible to distinguish a cipher from a random permutation. This can be done by querying the pairs of plaintexts with the difference $\Omega_P$ as in the characteristic and counting the number of pairs that arrive at the ciphertext difference $\Omega_C$ predicted by the characteristic. Such a distinguisher will use $O(p^{-1})$ pairs. Indeed, given $M = C/p$ pairs (for some constant (C > 1) chosen independently with the difference $\Omega_P$, the probability that no one of them will follow the characteristic is $(1-p)^M = (1-p)^{C/p} < e^{-C}$ which can be made arbitrarily small by choosing sufficiently large C. On the other hand the probability that $\Omega_C$ will not occur for similarly chosen pairs passed through a random permutation is $(1-2^{-64})^M$ . This probability is very close to one if $p >> C.2^{-64}$. However one can design even better attacks that can find the full secret key of a cipher. This can be done by considering differential characteristics which are by one, two, or N rounds shorter then the full cipher (the corresponding attacks are called 1R, 2R and NR-attacks respectively). This approach has two benefits: first of all, the characteristics that we use are shorter, and thus have higher probabilities; second, we can now analyze the final rounds of a cipher (which are not covered by the characteristic) by doing partial guesses of the secret key, performing partial decryption with these guesses and checking them against the prediction of $\Omega_C$. For example, suppose that as in 1R attack we know the output difference $(L', R')$ at the input to the last round. Denote the ciphertext halves by $C_L, C_R$ and their differences by $C'_L, C'_R$. Since the right half of the text is not altered and not switched, it means that $C'_R = R'$. This gives a 32-bit condition that helps to filter out many wrong pairs that do not follow the characteristic. Since we know the left half of the ciphertext difference $C'_L$ and $L'$ we can calculate the difference in the output of the F-function in the last round as $C'_L \oplus L'$. On the other hand we know the input to the F-function in the last round which is $C_R$. Thus for each S-box in the last round we know its output difference $S'_O$ and we know the exact values of its inputs up to XOR with six unknown bits of the last round subkey and thus also the input difference $S'_I$ to the same S-box. By checking the entry in the difference distribution table of the particular S-box corresponding to $S'_I$ and $S'_O$ we can write out all the possible six-bit pairs with input difference $S'_I$ that could cause the output difference $S'_O$.Comparing this list with the actual values which we know up to XOR with the subkey, we receive a number of guesses for a six bit portion of the last subkey [6]. Given several pairs that satisfy the characteristic we can further reduce the number of subkey guesses to the very few ones. Notice that the process described above can be performed independently for each S-box.

**Differentials vs. Characteristics**

Differential characteristic has a drawback of restricting differences in intermediate values which are rarely used in the actual differential attack. If there are many characteristics with equal input/output differences but following different intermediate paths these can be combined into a differential whose probability is the sum of probabilities of accumulated characteristics. In many modern ciphers studying differentials instead of characteristics brings a huge amplification of the probability. Here is a more formal definition of a differential [7]:

**Definition 4.** An *r*-round *differential* is a pair $(\Delta P, \Delta C_r)$, where $\Delta P = P \oplus P^*$ is the difference of plaintext and $\Delta C_r$ is the output difference at the $r^{\text{th}}$ round. The probability of an r-round differential is the conditional probability that given an input difference $\Delta P$ at the first round, the output difference at the $r^{\text{th}}$ round will be $\Delta C_r$, when the plaintext P and the subkeys $S_i$ are independent and uniformly random[7].

Also, the following idea of packing pairs into structures, suggested in [1] helps to decrease the data requirements of differential attack.

Suppose our attack can use successfully several linearly independent input differences $\delta_i, i = 1,...,k$, then for some plaintext $A$ we will require the ciphertexts of $A, A \oplus \delta_1, A \oplus \delta_2, A \oplus \delta_3, ..., A \oplus \delta_1 \oplus \delta_2, A \oplus \delta_2 \oplus \delta_3, ..., A \oplus \delta_1 \oplus \delta_2 \oplus \delta_3, ...$ .Then a pool of $2^k$ such ciphertexts contains $k.2^{k-1}$ pairs with differences from the set $\{\delta_1, ..., \delta_k\}$.

Differential cryptanalysis was significantly refined after its discovery: Truncated differential attacks, higher-order differentials, boomerang attacks.

When measuring the resistance of a cipher against differential cryptanalysis, only “basic” differential cryptanalysis is taken into account.

**Linear Cryptanalysis**. Linear cryptanalysis acts as a modeling the non-linear components of a cipher algorithm using the affine-linear approximations. In this model one starts by determining “good” linear approximations for individual components of the cipher, then builds an approximation for a single round from these and finally searches for a path through the cipher that makes use of the round approximations. By a “good” approximation, an affine-linear function approximating the original function with a probability $p = 0.5 + \varepsilon$ with $|\varepsilon|$ as large as possible is meant. This variable $\varepsilon$ is called the bias.

Linear cryptanalysis uses the bit masks to indicate which bits of the input and output are used in a linear approximation:

**Definition 5.** Let $(a,b) \in GF(2)^n \times GF(2)^n$ be a pair with $a \neq 0$ being the input mask and $b$ being the output mask. The linear probability for $(a,b)$ then is defined as

$$LP(a,b) = (2.\Pr_X\{\langle a, X \rangle = \langle b, \rho(X) \rangle\} - 1)^2 \tag{3}$$

Similar to the case of differential cryptanalysis, a vector of masks $A=(a_1,...,a_{r+1})$ with $a_i \neq 0$ for all $1 \le i \le r$ is called *linear characteristic* of a cipher[8].

Matsui proposed the following lemma, called Piling-Up Lemma:

**Lemma 6.** (Piling-up lemma). Assume $X_1,...,X_n$ are independent random variables representing bits and $\varepsilon_1,...,\varepsilon_n$ are their respective biases. We can then calculate the bias $\varepsilon$ of $X_1 \oplus ... \oplus X_n$ as follows[8]:

$$\varepsilon = 2^{n-1}\prod_{i=1}^{n}\varepsilon_i \tag{4}$$

Using Lemma 6, one can estimate the probability of success of a linear attack if the probabilities for individual approximations are known. Given the affine-linear expression approximating a cipher with probability $p$ we can expect to an attack using linear cryptanalysis to require $\approx p^{-2}$ known plaintext/ciphertext pairs.

### Interpolation Attacks

Interpolation attacks were presented in [5] as a reaction to ciphers using algebraically constructed S-Boxes such as those proposed by Nyberg [9]. In fact, interpolation attacks were the first demonstration of successful polynomial-based algebraic attacks against block ciphers. This attack works by expressing the relationship between the plaintext and ciphertext for a fixed key as either one or as a vector of polynomials.

The coefficients of the polynomials can be interpolated from a number of plaintext/ciphertext pairs because the degree of these polynomials is low enough. In [5] upper bounds on the data complexity – the number of required pairs for known-plaintext interpolation attacks – are given for selected examples. Courtois later improved on the work of Jakobsen and Knudsen and introduced an attack called General Linear Cryptanalysis [10]. In the same paper he also gives several examples of insecure ciphers based on inversion based S-Boxes that resist differential and linear cryptanalysis.

**Conclusion:** In this paper, we described previously known cryptanalytic techniques. It covers the different attack scenarios against ciphers which are known in literature, such as chosen key attack, related key attack and so on. We also explained the specific attacks on DES block cipher in more details.

# References

[1] Biham, E., Shamir, A. 1993. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, ISBN: 0-387-97930-1.

[2] Boneh, D., DeMillo, R. A., Lipton, R. J., On the importance of checking cryptographic protocols for faults, *Proceedings of Advances in Cryptology, EUROCRYPT 97*, Springer-Verlag, 1997; 1233: 37–51.

[3] Rezaeipour, D., Rushdan Md Said, M., The block cipher algorithm-properties, encryption efficiency analysis and security evaluation, *Journal of the Advances and Applications in Mathematical Sciences* 4(2): 129-137, 2010.

[4] Gosudarstvennyi standard 28147-89, Cryptographic Protection for Data Processing Systems, Government Committee of the USSR for Standards: 1989.

[5] Jakobsen, T., Knudsen, L., The interpolation attack on block ciphers, *Proceedings of 4th International Workshop on Fast Software Encryption, FSE 97*, Springer-Verlag, 1997; 1267: 28–40.

[6] Rezaeipour, D., Rushdan Md Said, M., The fundamental principles for security evaluation in block cipher algorithms, *2nd Extending Industrial Application of Information, Communications and Computations* (EIAICC 2013) *Conference*, Oct. 2013, Iran.

[7] Lai, X., Massey, J. L., Murphy, S., Markov Ciphers and Differential Cryptanalysis, *Proceedings of Advances in Cryptology, EUROCRYPT 91*, Springer-Verlag, 1992; 547: 17–38.

[8] Nyberg, K., Knudsen, L. R., Provable security against a differential attack, *Journal of Cryptology* 1995; 8: 27-37.

[9] Cid, C., Murphy, S., Robshaw, M. J. B., An Algebraic Framework for Cipher Embeddings. In *10th IMA International Conference on Coding and Cryptography*, Springer-Verlag , 2005; 3796: 278-289.

[10] Rezaeipour, D., Rushdan Md Said, M., The Vulnerability Analysis and the Security Evaluation of Block Ciphers", *International Mathematical Forum*, 5(42): 2071 – 2075 , 2010.

[11] Rijmen, V., Daemen, J., Preneel, B., Bossalaers, A., Win, E. D., The Cipher SHARK, *Proceedings of Fast Software Encryption: 3thInternational Workshop, FSE'96*, Springer-Verlag, 1996; 1039: 99–111.

[12] Rezaeipour, D., Rushdan Md Said, M., Some Statistical Simulation Results over the 128-bit Block Cipher CLEFIA, *International Journal of Contemporary Mathematical Sciences,* Vol. 4, no. 10, pp. 497 - 504. 2009

[13] Biryukov, A., The Boomerang Attack on 5 and 6-Round Reduced AES, *Advanced Encryption Standard 4th International Conference, AES 2004*, Springer-Verlag, 2005; 3373: 11–15.

[14] Knudsen, L. R., Truncated and higher order differentials, in *Fast Software Encryption ,FSE'94*, Springer-Verlag, 1995 ; 1008: 196–211.