DIFFERENTIAL CRYPTANALYSIS OF THE FULL 16-ROUND DES

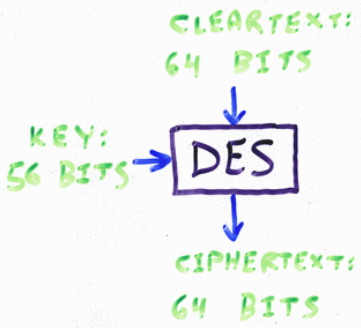
ADI SHAMIR
APPLIED MATH DEPT
THE WEIZMANN INSTITUTE
ISRAEL

(JOINT WORK WITH ELI BIHAM)

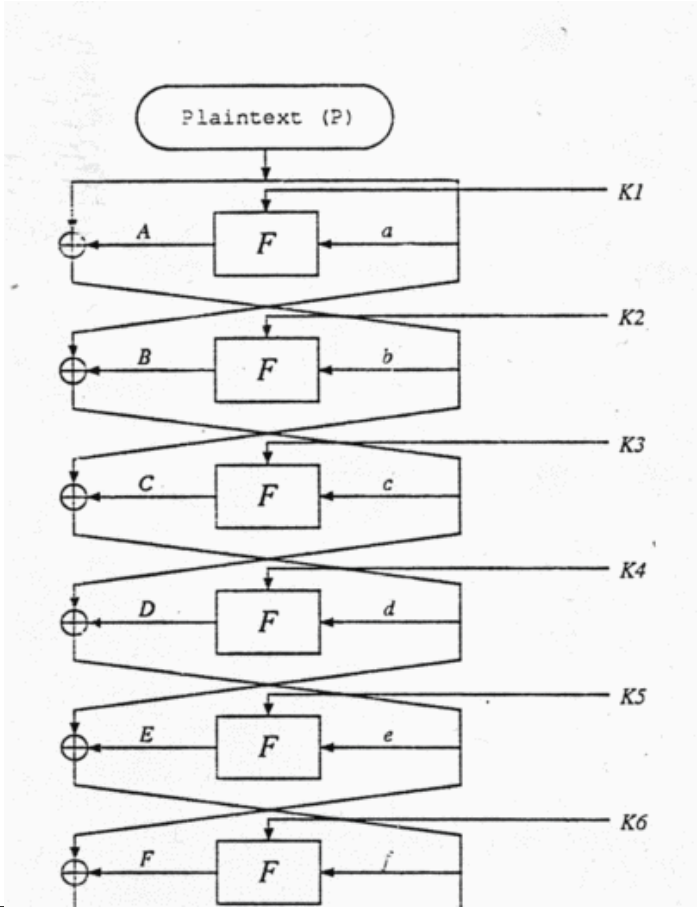
HISTORY OF THE DES

- DEVELOPED AT IBM IN EARLY 70's
- INCORPORATED NSA-SUPPLIED DESIGN CRITERIA
- ADOPTED BY THE NBS (NIST) IN 1977
- REAPPROVED EVERY 5 YEARS
- IN WIDE USE, ESPECIALLY IN BANKING APPLICATIONS.

DESCRIPTION OF THE DES



A BLOCK-ORIENTED CRYPTOSYSTEM WITH SEVERAL MODES OF OPERATION



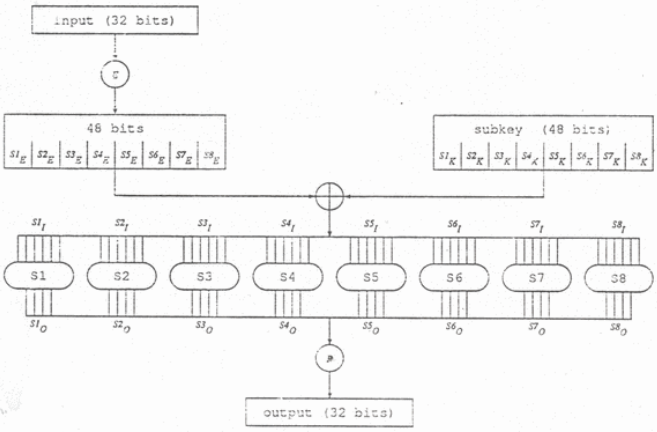


Figure 2: The F function of DES

BEHAVIOUR OF THE DES UNDER A MODIFIED CLEARTEXT:

SINGLE BIT CHANGED

CLEARTEXT

SAME KEY → DES

CIPHERTEXT

ABOUT HALF THE BITS ARE CHANGED

THE AVALANCHE PROPERTY

DES WITH FEW ROUNDS:

THE AVALANCHE IS LIKELY TO AFFECT ALL THE OUTPUT BITS AFTER ABOUT 4 ROUNDS.

CHAUM AND EVERTSE [1987] USED THIS TO ATTACK DES REDUCED TO 6 ROUNDS:

IN A "MEET IN THE MIDDLE" ATTACK, THE AVALANCHE IS INCOMPLETE IF WE GO FORWARDS 3 ROUNDS AND BACKWARDS 3 ROUNDS.

HOWEVER, THE SAVING IS ONLY A FACTOR OF 4 OVER 2^{56}

A FIXED MODIFICATION PATTERN OF BITS, P'

CLEARTEXT P

KEY → DES

CIPHERTEXT T

RESULTANT MODIFICATIONS

- WE ENCRYPT A RANDOM P TO GET T.
- WE MODIFY P BY THE FIXED PATTERN P', AND ENCRYPT THE RESULTANT $P^* = P \oplus P'$ TO GET T^*.

DIFFERENTIAL CRYPTANALYSIS EXPLOITS THE RELATIONSHIP BETWEEN $P' = P \oplus P^*$ AND $T' = T \oplus T^*$.

WHAT MAKES A PATTERN P' "GOOD"?

1. THE VARIOUS [redacted] INPUT BIT MODIFICATIONS SHOULD INTERFERE RATHER THAN ENHANCE THE RESULTANT OUTPUT MODIFICATIONS.
2. THIS BEHAVIOUR SHOULD BE INDEPENDENT OF THE CHOICE OF KEY.
3. THIS BEHAVIOUR SHOULD HAPPEN WITH A HIGH PROBABILITY.

KNOWLEDGE OF INPUT ⊕ IMPLIES KNOWLEDGE OF OUTPUT ⊕ EVERYWHERE IN THE DES EXCEPT AT THE S-BOXES (WHICH ARE THE ONLY NON-LINEAR PART OF THE SYSTEM).

- THERE ARE $64 \times 64 = 4096$ POSSIBLE PAIRS OF INPUTS TO THE S-BOX.
- THEY CAN BE GROUPED TOGETHER INTO 64 SETS, EACH HAVING A COMMON ⊕ VALUE.
- THE 64 PAIRS IN EACH SET HAVE 64 POSSIBLE OUTPUT ⊕, EACH BEING A 4-BIT QUANTITY.

THIS STRUCTURE IS SUMMARIZED IN A "PAIRS ⊕ DISTRIBUTION TABLE".

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
								⋮								
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
								⋮								
$3F_x$	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

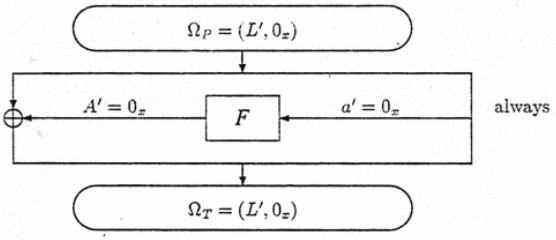
Table 2: Partial pairs XOR distribution table of S1

A CHARACTERISTIC IS A LABELING OF SOME CONSECUTIVE ROUNDS OF THE DES WITH ⊕'ED VALUES.

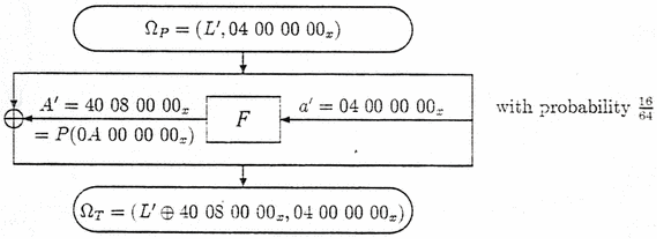
EACH CHARACTERISTIC HAS AN:

- INPUT ⊕
- OUTPUT ⊕
- PROBABILITY OF OCCURENCE FOR A RANDOMLY CHOSEN CLEARTEXT PAIR AND KEY.

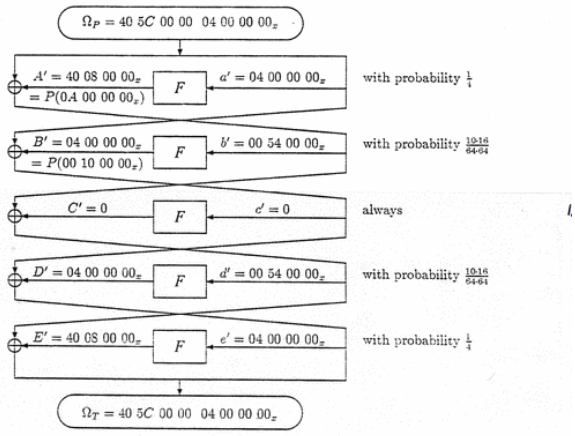
REMARK: THE PROBABILITY IS HARD TO COMPUTE DUE TO THE DEPENDENCE BETWEEN SUBKEY BITS, BUT IN PRACTICE EASY TO ESTIMATE DUE TO THE EXCELLENT RANDOMIZING NATURE OF THE DES.



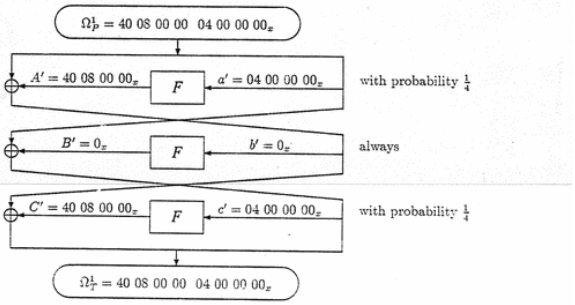
A one round characteristic with probability 1



A one round characteristic with probability $\frac{1}{4}$



The five round characteristic with probability about $\frac{1}{10000}$



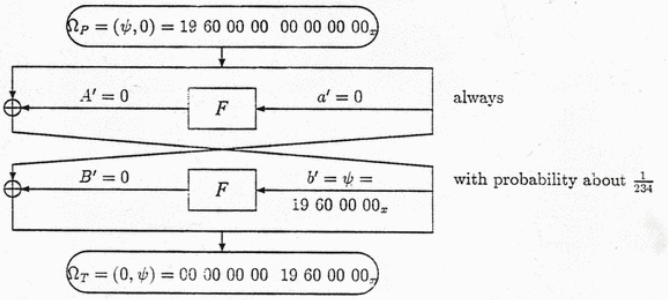
The three round characteristic with probability $\frac{1}{\ldots}$

ITERATIVE CHARACTERISTICS

WE WANT A STRUCTURED WAY TO CONSTRUCT GOOD CHARACTERISTICS OF ANY LENGTH.

TWO CHARACTERISTICS CAN BE CONCATENATED IF THE SWAPPED OUTPUT ⊕ OF THE FIRST IS EQUAL TO THE INPUT ⊕ OF THE SECOND. THE COMBINED PROBABILITY IS THE PRODUCT OF THE INDIVIDUAL PROBABILITIES.

AN ITERATIVE CHARACTERISTIC IS ONE WHICH CAN BE CONCATENATED WITH ITSELF (ARBITRARILY MANY



The iterative characteristic

HOW TO FIND GOOD CHARACTERISTICS

- INPUT ⊕'S WHICH CONTAIN MANY 1'S ARE UNLIKELY TO LEAD TO HIGH PROBABILITY CHARACTERISTICS.
- INPUT ⊕'S WITH A SMALL NUMBER OF 1'S CAN BE FOUND BY A COMPUTER SEARCH.
- GOOD CHARACTERISTICS CAN BE FOUND BY HAND SIMULATIONS AIDED BY SOME PLAUSIBLE HEURISTICS:

1. USE ONLY LARGE ENTRIES IN THE PAIRS ⊕ DISTRIBUTION TABLES.
2. USE ONLY 1'S WHICH ENTER ADJACENT S-BOXES.
3. LIMIT THE SEARCH ONLY TO STRUCTURES WHICH ARE ALLOWED BY THE KNOWN S-BOX DESIGN RULES.

THE OLD RESULTS (ANNOUNCED AT CRYPTO 90):

Rounds	Complexity (ciphertexts)	Memory (K bytes)	Time on PC (seconds)
4	2^4	-	-
6	2^8	100	0.3
8	2^{18}	460	120
9	2^{26}	≈ 100	
10	2^{35}	≈ 100	
11	2^{36}	≈ 100	
12	2^{43}	≈ 100	
13	2^{44}	$\approx 2^{20}$	
14	2^{51}	≈ 100	
15	2^{52}	$\approx 2^{32}$	
16	2^{58}		
Feal-8	2000	300	120
GDES	16	100	0.2

Table 1: Summary of the cryptanalysis of DES

OTHER OLD RESULTS (ANNOUNCED AT CRYPTO 90):

Results

DES with independent subkeys

1. Eight rounds are breakable as in dependent subkeys.
2. 16 rounds are breakable in 2^{61} (instead of 2^{768}) steps.

Weaker DES variants

3. DES with a changed order of the S boxes.
4. DES with addition operations instead of XOR operation.
5. DES with random S boxes or changed S boxes.
6. The modification of the P permutation by any other permutation or function cannot affect the results.

Feal-N

7. Feal-N with $N \leq 31$ rounds is breakable faster than exhaustive search.

Hash functions

8. Snefru with two pass is easily breakable.
9. The nHash variant with six rounds (instead of eight rounds) is easily breakable.

THE NEW RESULTS (DECEMBER 1991):

- WE CAN GET ONE MORE ROUND "FOR FREE".
- WE DO NOT NEED LARGE COUNTER ARRAYS
- WE CAN ATTACK SYSTEMS WHICH USE FREQUENT KEY CHANGES
- THE [redacted] ATTACK CAN BE APPLIED WITH ANY NUMBER OF CHOSEN CLEARTEXTS, WITH A LINEARLY GROWING PROBABILITY

- 2^{47} CHOSEN CLEARTEXTS ARE ENCRYPTED.
- 99.9 % OF THE CIPHERTEXTS ARE IMMEDIATELY ELIMINATED.
- THE REMAINING 2^{36} CIPHERTEXTS ARE ANALYSED IN 2^{37} TIME AND NEGLIGIBLE SPACE.
- THE ANALYSIS CAN BE CARRIED OUT ON A PARALLEL MACHINE.
- THE ANALYSIS CAN BE INCREMENTAL, E.G., WHEN 2^{29} CIPHERTEXTS ARE CHOSEN FROM 2^{40} CANDIDATES, THE ANALYSIS TIME IS 2^{30} AND THE PROBABILITY OF SUCCESS IS $\approx 1\%$

THE ORIGINAL DIFFERENTIAL ATTACK ON DES:

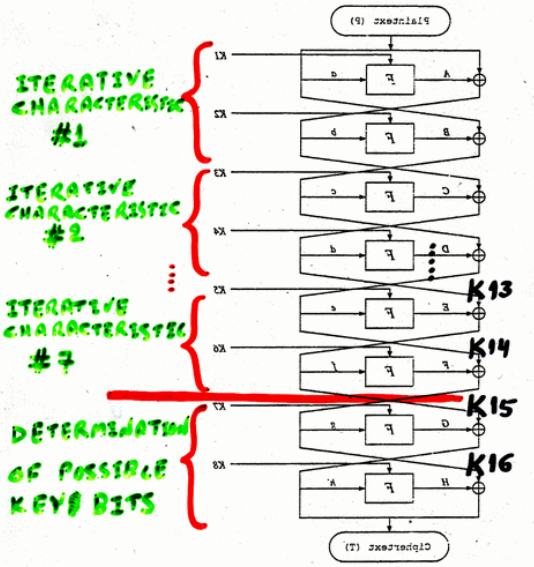


Figure 1: DES with eight rounds

PROBABILITY FOR 16 ROUNDS: $\left(\frac{1}{234}\right)^7 \approx 2^{-55}$

THE NEW DIFFERENTIAL ATTACK ON THE FULL 16 ROUND DES:

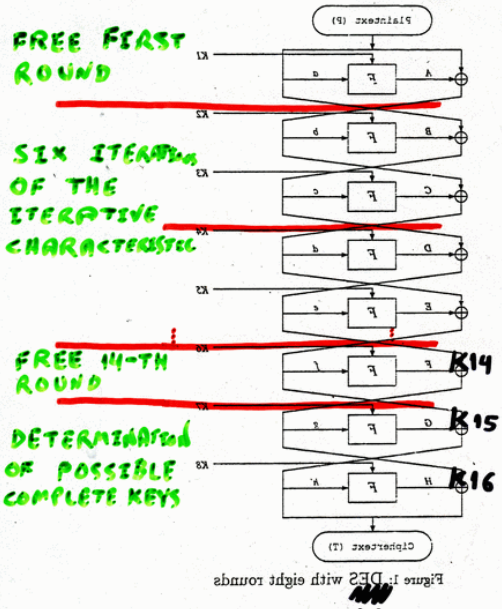


Figure 1: DES with eight rounds

TOTAL PROBABILITY FOR 16 ROUND DES:

THE ASSUMED ⊕ VALUES:

FREE FIRST ROUND

ALWAYS

PROB = $\frac{1}{234}$

ALWAYS

PROB = $\frac{1}{234}$

ALWAYS

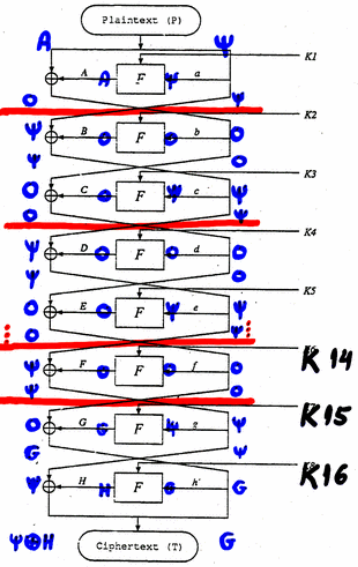


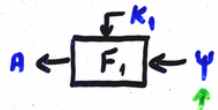
Figure 1: DES with eight rounds

16

HOW TO FIND THE PROPOSED KEYS

WE ASSUME THAT THE GIVEN PAIR OF CLEARTEXTS (P, P^*) WITH $P \oplus P^* = P' = (A, \Psi)$ IS A RIGHT PAIR, GIVING RISE TO ALL THE ASSUMED INTERMEDIATE ⊕ VALUES.

CONSIDER THE FIRST AND LAST ROUNDS:



ACTUAL INPUTS TO EACH S-BOX ARE KNOWN

ACTUAL INPUTS TO EACH S-BOX ARE KNOWN

64 POSSIBLE KEY VALUES ENTER EACH S-BOX. ABOUT 1/16 (4 VALUES) WILL PRODUCE THE ASSUMED ⊕'ED OUTPUTS, AND THUS $4^8 = 2^{16}$ KEYS ARE SUGGESTED BY EITHER F_c. HOWEVER, SINCE THE SAME BIT VALUES ARE USED IN BOTH F_1 AND F_{16}, THE KEY IS ALMOST UNIQUE.

Output XOR ($S1'_O$)	Possible Inputs ($S1_I$)
1	03, 0F, 1E, 1F, 2A, 2B, 37, 3B
2	04, 05, 0E. 11, 12, 14, 1A, 1B, 20, 25, 26, 2E, 2F, 30, 31, 3A
3	01, 02, 15, 21, 35, 36
4	13, 27
7	00, 08, 0D, 17, 18, 1D, 23, 29, 2C, 34, 39, 3C
8	09, 0C, 19, 2D, 38, 3D
D	06, 10, 16, 1C, 22, 24, 28, 32
F	07, 0A, 0B, 33, 3E, 3F

Table 5: Possible input values for the input XOR $S1'_I = 34_x$ by the output XOR (in hexadecimal)

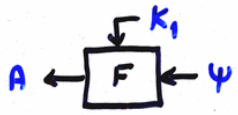
S box input		Possible Keys	
06,	32	07,	33
10,	24	11,	25
16,	22	17,	23
1C,	28	1D,	29

Table 6: Possible keys for $34_x \rightarrow D_x$ by S1 with input 1_x, 35_x (in hexadecimal)

S box input		Possible Keys	
01,	35	03,	37
02,	36	00,	34
15,	21	17,	23

Table 7: Possible keys for $34_x \rightarrow 3_x$ by S1 with input 21_x, 15_x (in hexadecimal)

HOW TO GET A FREE FIRST ROUND



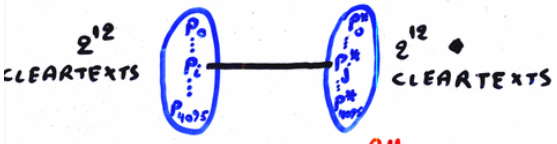
Ψ IS NON-ZERO ONLY AT THE INPUTS TO 3 S-BOXES, AND THUS A CAN BE NON-ZERO ONLY AT THEIR 12 OUTPUT BITS.

INSTEAD OF USING PAIRS OF CLEARTEXTS, WE CONSIDER STRUCTURES WITH 2^{13} CLEARS:

P = RANDOM 64-BIT CLEARTEXT

$P_i = P \oplus (V_i, 0)$ $\quad P_j^* = P \oplus (V_j, \Psi)$

WHERE $V_0, V_1, \cdots, V_{4095}$ ARE ALL THE POSSIBLE VALUES AT THOSE 12 OUTPUT BITS.



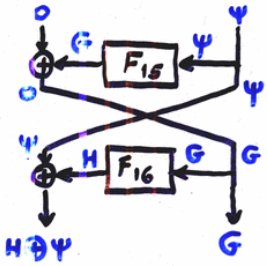
24

WE CONSIDER THE 2^{24} PAIRS (P_i, P_j^*) WITH $\oplus$: $P' = (V_i \oplus V_j, \Psi) = (V_k, \Psi)$, WHERE EACH V_k OCCURS EXACTLY 2^{12} TIMES.

HOW CAN WE QUICKLY FIND THE RIGHT PAIRS AMONG THE 2^{24} $\oplus$'S ?

TRYING ALL OF THEM WILL MAKE THE ATTACK SLOWER THAN EXHAUSTIVE SEARCH

HOWEVER, IN THE LAST TWO ROUNDS WE HAVE:



Ψ IS NON-ZERO ONLY AT 3 S-BOX INPUTS, AND THUS G IS ZERO AT 20 BITS. SINCE G IS VISIBLE AT THE OUTPUT, ONLY 2^{-20} OF THE 2^{24} PAIRS ARE LIKELY TO PASS THIS FILTER, WHILE THE COST OF APPLYING THE FILTER IS JUST 2^{12}.

HOW TO FIND THE $2^4 = 16$ INTERESTING PAIRS:

- SORT (OR HASH) ALL 2^{13} MESSAGES BY THE 20 RELEVANT BITS (WLG, ASSUME THAT THESE ARE THE 20 MOST SIGNIFICANT BITS).
- EACH POSSIBLE 20-BIT VALUE OCCURS WITH 2^{-7} PROBABILITY, AND THUS MULTIPLE OCCURRENCES ARE VERY RARE.

- SCAN THE SORTED LIST AND EXTRACT ALL THE P_i, P_j^* PAIRS FROM EACH MULTIPLE OCCURENCE OF SOME 20 BIT VALUE.
- FINDING THE ~16 PAIRS OUT OF THE 2^{24} CANDIDATE PAIRS TAKES ONLY 2^{13} TIME.

NEW DEVELOPMENT:

IN MAY 1993, MITSURU MATSUI FROM MITSUBISHI LABS, JAPAN, ANNOUNCED A NEW KNOWN MESSAGE ATTACK ON THE FULL 16 ROUND DES WHOSE COMPLEXITY IS ALSO 2^{47}.