How easy is collision search. New results and applications to DES

(abstract and results)

Jean-Jacques Quisquater & Jean-Paul Delescaille

Philips Research Laboratory Brussels
Avenue Van Becelaere, 2; Box 8
B-1 170 Brussels, Belgium
ijq@prlb.philips.be — jpdesca@prlb.philips.be

1 Update about collisions in DES

Given a cryptographic algorithm f (depending upon a fixed message m and a key k), a pair of keys with collision k_0 and k_1 (in short, a *collision*) are keys such that

$$f(m, k_0) = f(m, k_1).$$

The existence of collisions for a cryptographic algorithm means that this algorithm is not *faithful* in a precise technical sense (see [2]).

An efficient algorithm (called algorithm 1 in the tables) was used on a network of workstations (thirty SUN's and ten microVAXes) for finding pairs of keys with collision in the DES. The algorithm is based on the so-called theory of *distinguished points* (see [3], [4]) and is described in [4]. Table 1 gives the set of 26 collisions found with the same plaintext 0404040404040404.

The same algorithm was used to find a collision when using a double DES in encryption mode (with 2 distinct keys, k and k') with the same fixed plaintext. Table 2 gives one such a collision.

2 Meet-in-the-middle attack

The *meet-in-the-middle attack* is the finding of a pair of keys k, k' such that

$$f(f(m_0, k), k') = m_1$$

where f is again the DES in encryption mode and m_0 and m_1 are fixed messages.

The classical meet-in-the-middle attack is based on the computations of $f(m_0, k_0)$ for 2^{32} distinct keys and the same number of computations for $f^{-1}(m_1, k_1)$; then a common value is likely (the birthday paradox) found by sorting the two obtained sets. One problem is to store 2^{33} values of 8 bytes. Here instead of storing each computed value, we only store distinguished points (output values with 11 zeroes at the left) from the two sets: we need more output values (and thus more computations) for

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 408-413, 1990.

finding a common value but less memory. The output values were computed using the same strategy than for the algorithm 1: that is, we found new collisions during the process. Table 3 gives the 22 found collisions when the plaintext is "WELCOME ". Table 4 gives the 31 found collisions when the ciphertext is "CRYPTO89" and DES is used in decryption mode.

The common value was found a specific algorithm using hashing tables. The full paper will explain the strategy we use. Table 5 gives the value found during the first effective meet-in-the-middle attack. Let us notice that the common value has 11 *predetermined* bits set at 0.

3 Other results

We also used a variant of algorithm 1 (named algorithm 3 in the tables) both for finding collisions and for the meet-in-the-middle attack. This variant consists to replace in algorithm 1 (see [4]) the iteration $y \leftarrow f(m,y)$ by $y \leftarrow f_{bit_\ell}(m_\ell, y)$ where bit_ℓ is the ℓ-th bit of y, with ℓ fixed; the functions f_0 and f_1 are respectively the DES in encryption mode with the plaintext "WELCOME " and the DES in decryption mode with the ciphertext "CRYPTO89", for this application. This idea was independently found by Coppersmith ([1]). Table 6 gives 4 new collisions. Table 7 gives 2 new meet-in-the-middle attacks.

References

[1] Don Coppersmith, *Mathematical foundations of cryptography*, 1989, in preparation.

[2] Burton Kaliski, Ronald Rivest and Alan Sherman, *Is the Data Encryption Standard a group? (Results of cycling experiments on DES)?*, J. Cryptology, vol. 1, 198, pp. 3–36.

[3] Jean-Jacques Quisquater and Jean-Paul Delescaille, *Other cycling tests for DES*, Springer Verlag, Lecture notes in computer science **293**, Advances in cryptology, Proceedings of CRYPTO '87, pp. 255–256.

[4] Jean-Jacques Quisquater and Jean-Paul Delescaille, *How easy is collision search. Application to DES*, Proceedings of EUROCRYPT '89, To appear.

Table 1. Collisions (k_0, k_1) found in DES (mode encryption) with fixed plaintext = 0404040404040404, using algorithm 1.

k0	k1	plain	cipher
46b2c8b62818f884	4a5aa8d0ba30585a	0404040404040404	f02d67223ceaf91c
1680b00c1c22c6b4	d296c2ca66be3c60	0404040404040404	e20332821871eb8f
22a64edc20e07032	6edaa03254d2a298	0404040404040404	7237f9e44466059f
620e08e886aa8c1c	cc3adc3616cc1c32	0404040404040404	345d8975676ffde0
b41ebe7a88c4a8c8	a2aa9adc56a60ad6	0404040404040404	301c9a64b903048d
8654a2b862a82486	5888c640ee3016d4	0404040404040404	8f4a67da0852722d
0ed86014328cf2da	1e620c46682e325c	0404040404040404	96f0faf4f80b6b29
92f69c5aa2c84ee8	780a76586c7c0ca4	0404040404040404	1d901196097a93f4
1680f2049484b4b2	46f422a832ac0c18	0404040404040404	85795a73b4af5d78
e4f06aaea2022e02	3eb8406c969c9c84	0404040404040404	46184d44b739a147
36a0f03afe48c226	28e8161878343ea0	0404040404040404	c5ed963b29a48bf6
5c4afa4ae0c62a84	060c0e048614bc42	0404040404040404	c931dab489f515a1
d8fc6cba3c0a946c	d0e4aa90baba681c	0404040404040404	a3c7d6d33eb1400d
2c2c5a243cd882fa	36da7e6010d6a07e	0404040404040404	6a5d431ed4863421
ac78ca74c6a0ea6e	7aac9c602e9854b6	0404040404040404	2edeaaa86e5141af
ae8838904874c606	ce806eee7cfcd2ec	0404040404040404	150e0b6ff35b4f0e
76f6527c54447ade	366cf4baa8cc6c80	0404040404040404	77964b1e86be688e
be827240c8bc3e6a	6ece1e20bef2b0f8	0404040404040404	f29fdbc8dc6c174a
5406c60cb4d6f0c8	5e301c2452d88476	0404040404040404	c6120f53b62eed0d
b45e08326ea40e10	0e5ebe562c961274	0404040404040404	ef5293f14f84fc4f
a862d2aef0c06c54	624e36aa48926a2e	0404040404040404	7dd3c3d34ea30c2f
02e6f2c46a40ba0e	125eb8b03c589c54	0404040404040404	3af6bac78416503d
1c3a0ed4f4cca240	bee020625838006a	0404040404040404	2b1331f0ae189c68
e0127ea26e0a9c80	6a3e00f268f0c4f6	0404040404040404	69e7467667b85945
f4c84030841492cc	72c6000236321cbe	0404040404040404	5db67a19b33fc3ab
4ceaf854e44a0a8e	a6367c24c0c8c258	0404040404040404	677277df7822abbf

Table 2. Collision $(k_i, k_i'), i = 0, 1$, found in *double* DES (mode encryption) with fixed plaintext = 0404040404040404, using algorithm 1.

i	k i	k' i	plain	cipher
0.	a6daeac810281cfa	1068d04ed4acbc3c	0404040404040404	b8c78d848dcc1a64
1.	aaa2bcda8c40ca5e	d21476e4b69466be	0404040404040404	b8c78d848dcc1a64

Table 3. Collisions (k_0, k_1) found in DES (mode encryption) with fixed plaintext "WELCOME␣" (in hexadecimal) during use of algorithm 2.

k0	k1	plain	cipher
9ae23a0c4c8a226e	b68858b28a6eae32	20454d4f434c4557	8c94880b085330c7
3af8987236e69410	0cc8a6cc46c442be	20454d4f434c4557	bae455f4f9825466
e00a7ce87c56668a	d2fa5cb4461a7036	20454d4f434c4557	2ddee611bd255625
708ce29a6662443a	d032fc7e5cece010	20454d4f434c4557	9f989601e97eea08
ccb246c24ceec4c0	fac6b210a0a0e66e	20454d4f434c4557	9bdfd47aa8765800
8c42ec6ce2968230	669eaabcdabca6e4	20454d4f434c4557	f1b9c371cb484fbd
840ee66a505e00a6	3e1a36600a08925c	20454d4f434c4557	f4210871ad57427a
70bab4769a2c5254	fe866cac0c4a3248	20454d4f434c4557	684cb0a558dedea9
c4d63aec50745c16	e4949a3ab288d4f0	20454d4f434c4557	3886c01aad1ceb09
5ccc388c468e1c20	46c42a823c746836	20454d4f434c4557	d5944d3a27a8be52
76b65c8c84fabe32	9a86b298d880ec1a	20454d4f434c4557	56d73aa99035444b
c09020b4988c085e	464488de18746a24	20454d4f434c4557	e8a6d4d4b3d62ddf
f2f6da5256ec74a2	bae2e4da3890d416	20454d4f434c4557	8ae91121e209f9e8
fcbc7ee6cc3e9254	90b88a08041e969a	20454d4f434c4557	87057985fb756003
92908280a4e23a78	ce2492885e48f670	20454d4f434c4557	e43be5d1d51a4ac9
dab83c0c56108ae2	64207cb054da746a	20454d4f434c4557	f9c33b251a5ec47b
7894ee4a721a4482	6e6e1874e6daf018	20454d4f434c4557	85048af612532963
ca82c8fc1e54bed6	42202ed48c5c0aae	20454d4f434c4557	c9666f42a86b968e
e6f428e470ac2e7e	c8828266646a9e32	20454d4f434c4557	71f9208a9547a8b1
8658c486b81894c4	08641cfe966c4064	20454d4f434c4557	afe5c27ed0b2d778
52b6c8e46c32d0d2	e852448260688a8a	20454d4f434c4557	35c3c1252413d072
3c600e2cb6a404b6	8402b48c48882e36	20454d4f434c4557	b8c97f4ece12c6f2

Table 4. Collisions (k_0, k_1) found in DES (mode decryption) with fixed cipher "CRYPTO89" (in hexadecimal) during use of algorithm 2.

k0	k1	plain	cipher
02800e14b49ee86e	1280448278408620	4c1ad155fbc14716	39384f5450595243
5e9476e0ea2e4ab0	96fe66dce89c3448	3af999c9e1058c54	39384f5450595243
04b2a4a2e21a40a2	e0680ad6fa58487c	de348d105fc37ab3	39384f5450595243
0884a0d264025496	928e6e5a6e1a604c	4a6d235062f7e190	39384f5450595243
1e302c1666d8c280	3622cadee6ea7e78	88985912677cdbc3	39384f5450595243
70e45cc4803eec28	560050de5ea6dcc6	6eefe5e81c0e4af9	39384f5450595243
100ce63c74d4a2cc	30c8c818429ce6fe	6ca608fd45504b76	39384f5450595243
06f24006105a80b4	0052b616145aca40	2c375311e776aa97	39384f5450595243
da5ce25a84707208	7038e67080107434	b465c16b7d3a5ef3	39384f5450595243
3c781edce2b428c8	26e6b44894aab866	8e185a3b82633e3c	39384f5450595243
b2b2c814ac1ea2b6	ca963a306ee86eda	27b00453e16dd132	39384f5450595243
3042d4f8e4185e80	de62d4120a94302e	aa9489ba55276236	39384f5450595243
24e86a486e28ae60	926894b89e5ae0fa	f308907f59a2f273	39384f5450595243
1c2e66da5a46523c	fe42884ab83622c8	76f268301f944e6e	39384f5450595243
5a6a38386628560e0	42cca4ccc4665846	2a5b57ec38d95b1a	39384f5450595243
dc604826a476042a	4ce62014a8cc141e	4da1409fe4f97098	39384f5450595243
c0b0520a200cf004	4e8a5442c092f6b2	a09ad87ef26962bf	39384f5450595243
5e88d0487aeac8b0	5c045c842a16c076	c513e925a73ce3ca	39384f5450595243
9ed6d874106c6a0e	9eeefeda7c30823a	a91e0ad2717c5165	39384f5450595243
a62458ec32186260	beb06aa4e69a9c0a	32e338ccc8f61304	39384f5450595243
eab474b62276060e	e6e862c42cfa08c8	da8469d3f789170f	39384f5450595243
900ed69cf8e2dafe	fe222e58c072aa7e	e5a9587ee976d768	39384f5450595243
aadc88468e466898	32588a922844f2d4	49f386509b43490c	39384f5450595243
78b61a009444de6a	8004349e4a90306a	392269f09bf3056c	39384f5450595243
8e86e8946cfad0a2	60d858b8b8da6ac8	5617f9c377565524	39384f5450595243
e2a6f6d492389646	06365e0c464a7a40	697451d10c2a52f5	39384f5450595243
2284841e347cd2e8	bea4f09c62604830	702241d5ebb242f9	39384f5450595243
9a6260c48068e68e	98488cf6d85accd8	4bf50ce58bce531e	39384f5450595243
a22ef8d4beb28460	1ee4683e687cba34	2089ef2739e30ace	39384f5450595243
e45ec2f294187830	54003c400c5a6cf8	e5076d5fb1c6c97f	39384f5450595243
c010844e4a3030ec	363ee0f0fe0c9aa0	108c44a64de03689	39384f5450595243

Table 5. Meet-in-middle "attack" (k, k') against *double* DES (mode encryption) with fixed plaintext "WELCOME␣" (in hexadecimal) and fixed ciphertext "CRYPTO89" (in hexadecimal), using algorithm 2.

k	k'	plain	cipher
9a86e458dce6c46a	f2dc6822b028069e	20454d4f434c4557	39384f5450595243

Table 6. Collisions (k_0, k_1) found in DES (mode encryption) with fixed plaintext "WELCOME␣" (in hexadecimal), using algorithm 3.

k0	k1	plain	cipher
e24a2ca412be62ec	ca225aa270ac4e36	20454d4f434c4557	c0ee4acf421d8c16
2868be64201c12de	42d4d460105adc8c	20454d4f434c4557	e3d78af2e104a331
86a41682ea02a43a	3a8c9856848696de	20454d4f434c4557	a567b1c48dd5f045
4260fed06c5090e4	e01a788492d2f46a	20454d4f434c4557	5cc665796edb52ad

Table 7. Two other meet-in-the-middle "attacks" and collision $(k_i, k_i'), i = 0, 1$, found for *double* DES (mode encryption) with fixed plaintext "WELCOME␣" (in hexadecimal) and fixed ciphertext "CRYPTO89" (in hexadecimal) using algorithm 3.

i	k i	k' i	plain	cipher
0.	4a445612aa58e264	ca7e4098dc243818	20454d4f434c4557	39384f5450595243
1.	f4a2ce847e08886a	f2e2288aeae2b6fa	20454d4f434c4557	39384f5450595243