Quasigroups and Related Systems **14** (2006), 191 – 194

The application of DES, IDEA and AES in strong encryption

Czesław Kościelny

Abstract

The concept of strong encryption by means of DES and IDEA in [9, pp. 295, 324] has been mentioned. In the paper this thought concerning the commonly used DES, IDEA and AES algorithms has been developed and generalized.

1. Introduction

It has been announced in [2] that
... the Data Encryption Standard became effective July 1977. It was reaffirmed in 1983, 1988, 1993, and 1999. The DES has now been withdrawn. The use of DES is permitted only as a component function of TDEA, and that
with the withdrawal of the FIPS 46-3 standard:
1. Triple DES (i.e., TDEA), as specified in ANSI X9.52, Keying Options 1 and 2, is recognized as the only FIPS approved DES algorithm.
2. Other implementations of the DES function are no longer authorized for protection of Federal government information.
Note: Through the year 2030, Triple DES (TDEA) and the FIPS 197 Advanced Encryption Standard (AES) will coexist as FIPS approved algorithms - thus, allowing for a gradual transition to AES. (The AES is a new symmetric based encryption standard approved by NIST.)

In the light of the presented paper the above decision seems to be irrational because the protection of data by means of the Triple Data Encryption Algorithm is much more weaker than that offered by DES, used according to the method discussed in this work.

The paper is addressed to application researchers well acquainted with the standards [1], [4] and with the IDEA [3].

2000 Mathematics Subject Classification: 68P25, 94A60, 11T71
Keywords: DES, IDEA, AES, block ciphers, strong encryption

2. DES, IDEA and AES as a reason of contention

DES, IDEA and AES belong to a class of iterated block ciphers involving the sequential repetition of a round function and a particular subkey for each round. For any iterated block cipher encryption procedure is described by means of the equation

$$C = E(ks(K), M), \tag{1}$$

where E denotes two-variable encrypting function, $K-$ a secret key chosen by the user, and $M-$ a message to be encrypted. The secret key K is not directly applied in the encryption operation, but it serves as input data for the function ks, generating a key schedule, i.e. subkeys for each iteration. A number of cryptologists suspect that the function ks intends to "inject" into the cryptogram as much additional information about bits of the secret key K as possible during the encryption process instead of maximizing the diffusion and confusion. This additional information may deliver – to the privileged circle of the initiated – a manner of deciphering cryptograms without the knowledge of the secret key. To verify the justness of this suspicion one ought to find and analyze an explicit function F, which, taking into account both the encryption and key schedule generation algorithms, will allow to express symbolically the cryptogram

$$C = F(K, M), \tag{2}$$

and to compute it in one step, using the secret key K and the message M. But in the case of the iterated block ciphers this task is almost unfeasible.

The author shows in next section how to eliminate this bone of contention.

3. DES–768, IDEA–832, and AES–1408:1664:1920

It has been verified by the author that it is possible to encrypt data using the DES with the 768-bit key, IDEA with 832-bit key and bringing into play the AES with the key length equal to 1408 bits, 1664 bits or 1920 bits. In the case of the strong version of these algorithms the encrypting/decrypting procedures exactly conform to standards [1] and [4]. To transform DES and AES into strong ciphers it simply suffices to eliminate the key expansion algorithms, i.e. to generate arbitrarily the set of subkeys K_s for all iterations and to use it as a secret key. Then, applying the same encrypting algorithm E as in (1), we now compute the cryptogram of the message M according

to

$$C = E(K_s, M), \tag{3}$$

and we are sure that all bits of our modified secret key K_s participate in the encryption process. Thus, since DES needs sixteen 48-bit subkeys, in this way we will obtain the 768-bit secret key to protect a 64-bit block of data. The IDEA needs fifty two 16-bit subkeys for protecting 64-bit plaintext block - it means that the modified secret key for this algorithm can contain 832 bits. Similarly, AES−128, AES−192, AES−256, apply eleven, thirteen and fifteen 128-bit subkeys for encrypting a 128-bit message block, respectively. Making use of these sets of subkeys as secret keys we can now safeguard a 128-bit block of data with secret keys of 1408, 1664 and 1920 bits.

4. Strong symmetric-key block ciphers related to DES and to AES

Introducing small changes into the considered cryptographic algorithms we can further strengthen their protecting power. Discussing DES from this point of view we can treat the initial permutation IP, primitive functions $S_1 - S_8$ (S-boxes), permutation P and selection function E as variables and in this way enlarge additionally the key space. Since there can be

- $x = 64!$ permutations IP,
- $y = (4 \cdot 16!)^8$ sets of 8 S-boxes,
- $z = 32!$ permutations P,
- $u = 2^{40}$ selection functions E,

then the increase of a secret key length will be

$$\Delta_{DES} = \lfloor \frac{\ln(x \cdot y \cdot z \cdot u)}{\ln(2)} \rfloor, \tag{4}$$

that is 1591 bits. Thus, taking into account the previous section, we can use DES for protection 64-bit data block with key containing 2359 bits.

Some aspects of strong AES encryption have been already considered in [6]. In the instance of AES, we can get any from 30 irreducible polynomials of degree 8 over $GF(2)$ to compute in $GF(256)$. The transformation `SubBytes()` may be replaced by any permutation of 256 elements, one can replace `ShiftRows()` and `InvShiftRows()` transformations by a pair of random mutually invertible permutations acting on elements of the `State` array, and `MixColumns()` and `InvMiColumns()` transformations by a pair

of random mutually invertible 4 x 4 non-singular matrices over $GF(256)$. In this manner we can get the full protecting power of the AES (with the secret key up to 3736 bits).

5. Conclusions

In the paper an important application-oriented problem concerning the data security, has been presented. The author hopes that this work may have some influence on the future standardization policy in cryptography.

The method presented, with regard to IDEA, may be exactly tested by the reader by means of the `topicIDEA` Maple 10 package [7] available in the Maple Application Center. The author also worked aut `StrongDES` and `genericAES` Maple 10 packages more interesting from the point of view of teaching and research than the latter, allowing the reader to test the presented method in the case of DES and AES and to explore precisely these algorithms.

References

[1] **NIST**: *Data encryption standard (DES)*, FIPS PUB 46-3, October 1999

[2] **W. C. Barker**: *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, NIST Special Publication 800-67, May 2004

[3] **X. Lai and J. Massey**: *A proposal for a new block encryption standard*, Damgard, editor, Advances in Cryptology Eurocrypt'90: Workshop on the Theory and Application of Cryptographic Techniques, Aarhus, Denmark, May 1990, Proceedings, volume 473 of Lecture Notes in Computer Science, Springer-Verlag, 1991

[4] **NIST**: *Advanced Encryption Standard (AES)*, FIPS PUB 197, 2001

[5] **B. Schneier**: *Applied Cryptography*, (Second Edition): Protocols, Algorithms, and Cource Code in C, John Wiley & Sons, 1996.

[6] **C. Kościelny**: *AES with the increased confidentiality*, Quasigroups and Related Systems **13** (2005), 265 – 268.

[7] **C. Kościelny**: *The* `topicIDEA` *package*, January 2006
`http://www.maplesoft.com/applications/`

Received January 29, 2006

Academy of Management in Legnica, Faculty of Computer Science, ul. Reymonta 21, 59-220 Legnica, Poland
and
Wrocław University of Applied Informatics, ul. Słubicka 29-33, 53-615 Wrocław, Poland
E-mail: c.koscielny@wsm.edu.pl