SpeedyDes3 - Speedy Des3 Encryption for Video Poker Game Machines Licensed in Italy

K.L. Man, M. Mercaldi and H.L. Leung [*]

Abstract— **This paper presents our industrial experience on the implementation of SpeedyDes3 encryption which is a speed up version of the Des3 encryption. This SpeedyDes3 encryption improves the standard Des3 encryption by means of speed and memory usage. Our SpeedyDes3 encryption is particular suitable for use/running in small systems. We have applied the SpeedyDes3 for the encryption of data in video poker game machines licensed in Italy.**

Keywords: Des, Des3, SpeedyDes3, encryption, cryptography, video poker game machines

1 Introduction

Personal and company's data/information are extremely valuable and must be protected, both in operation and in physical file format. Nowadays, *cryptography* is used in many security applications present in our society. Such applications include the security of ATM cards, computer passwords, and electronic commerce, etc.

In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as ciphertext). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. "software for encryption" can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).

Encryption has long been used by militaries, banks and governments to facilitate secret communication. Encryption is now used in protecting information within many kinds of civilian systems, such as computers, storage devices (e.g. USB flash drives), networks (e.g. the Internet e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. Encryption is also used in digital rights management to prevent unauthorised use or reproduction of copyrighted material and in software also to protect against reverse engineering. (WIKIPEDIA - Encyclopedia [1])

Among various encryptions, the *Data Encryption Standard* (Des) [2] and the *Triple Des* (Des3) [3] are the two most popular encryptions. In this paper, we report on our implementation of the SpeedyDes3 encryption which is a speed up version of the Des3 encryption. Our SpeedyDes3 encryption improves the standard Des3 encryption by means of speed and memory usage. Also, the SpeedyDes3 encryption is particular suitable for use/running in small systems. We have applied the SpeedyDes3 for the encryption of data in video poker game machines licensed in Italy.

The reminder of the paper is organised as follows. Section 2 gives a brief overview of Des and Des3 encryptions. SpeedyDes3 encryption is introduced in Section 3. Commercial applications of SpeedyDes3 encryption are presented in Section 4. Finally, concluding remarks are made in Section 5.

2 Overview of Des and Des3

The Des was developed originally by an IBM team around 1974 and the Des3 is a variant of the standard Des which is approximately three times slower than the regular Des but offers major security benefits and coverage (than standard Des).

The Des is a cipher which is a method for encrypting information. It is based on a *symmetric-key* encryption that uses a 56-bit key. More specifically, Des takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations (e.g. Feistel function [3]) into another ciphertext bit-string of the same length.

The block size of Des is 64 bits and Des also uses a key to customise the transformation in such a way that decryption can supposedly only be used by those who know the particular key applied for encryption. The input key for Des is 64 bits long, the actual key used by Des is only 56 bits in length as other eight are used solely for checking parity, and are thereafter discarded (i.e. the actual key used by Des is only 56 bits in length).

In simple words, Des3 is a block cipher formed from the Des cipher by using it three times. Des3 generally operates as follows: $\mathrm{DES3} = \mathrm{DES}(k_3; \mathrm{DES}(k_2; \mathrm{DES}(k_1; \mathrm{M})))$, where DES3 is the Des3 encryption operation, DES is the

[*] K.L. Man and H.L. Leung are with Solari - Hong Kong, emails: systemcfl@gmail.com and sales@solari-hk.com. M. Mercaldi is with the M.O.S.T., Turin, Italy, email: michele.mercaldi@most.it.

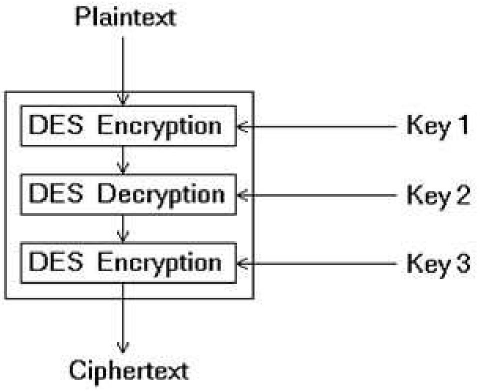

Figure 1: Triple Des Encryption (Des3)

Des encryption operation, M is the message intended to be encrypted and k_1, k_2 and k_3 are Des keys.

Usually, the middle step of DES3 is replaced with decryption so that $\mathrm{DES3} = \mathrm{DES}(k_3; \mathrm{DES}^{-1}(k_2; \mathrm{DES}(k_1; \mathrm{M})))$. Hence, a single Des encryption with key k can be represented as $k_1 = k_2 = k_3 = k$. Note that the choice of decryption for the middle step does not affect the security of the algorithm. Des3 allows for the use of one, two or three keys. Clearly, using three distinct keys is the most secure operation. Figure 1 depicts the Des3 encryption.

3 SpeedyDes3 Description

The implementation of SpeedyDes3 was inspired by [4] and the Italian administrative rules for video poker game machines[1]. Des3 encryption principally executes into 2 steps:

1. creation of a set of subkeys starting from the encryption key;
2. encryption involving a series of bit permutations based on input blocks of 64 bits and the created subkeys.

More precisely, Des3 encryption starts from a set of 3 keys of 64 bits. Based on the set of 3 keys, 48 subkeys are further created with 16 bits long for each key so that SpeedyDes3 is capable to reuse the same subkeys derived from the main keys. Such subkeys without further changes are used for the whole SpeedyDes3 encryption process. Due to this (using the same subkeys), memory usage is reduced remarkably and the runtime performance has increased multifold. In simple words, the development of SpeedyDes3 aims to improve the performance of the existing Des3 encryptions in terms of speed and memory usage which is also portable to run it on small systems (e.g. video games).

4 Applications: Video Poker Game Machines Licensed in Italy

Game machines, such as slot machines and poker game machines, that pay back tokens, such as coins, for winning game results have been very popular. Hence, encryption of game machine data (e.g. the winning game results) is one of the most important issues much interested by the tax offices/governments. Furthermore, two important issues needed to be considered for the application of SpeedyDes3 (to poker game machines) are the video game speed and the interaction between the game machine and the user. These two issues become more critical as the poker game machines are systems with limited resources (e.g. CPU speed and memory).

As SpeedyDes3 is specifically designed for running on small systems, we have applied the SpeedyDes3 for the encryption of data of a series of video poker game machines licensed in Italy whose have 20KB of Ram, 256KB of flash memory and the CPU of 10MHz. It has turned out that the SpeedyDes3 encryption was faster.[2]

5 Conclusions

In this paper, we have presented the SpeedyDes3 encryption which is a speed up version of the Des3 encryption. As commercial applications, we have applied the SpeedyDes3 for the encryption of data in video poker game machines licensed in Italy.

Our experience shows us that the SpeedyDes3 encryption outperforms the standard Des and Des3 encryption by means of speed and memory usage. In addition, the SpeedyDes3 encryption is particular suitable for use/running in small systems.

Acknowledgement

Many thanks go to the sponsor Electronic Center - Italy (http://www.el-center.com) of the presented work in this paper.

References

[1] Wikipedia, *http://en.wikipedia.org/wiki/Encryption.*

[2] Wikipedia, *http://en.wikipedia.org/wiki/Data_Encryption_Standard.*

[3] Wikipedia, *http://en.wikipedia.org/wiki/Triple_DES.*

[4] *Richard Outerbridge's public domain D3DES library,* Copyright (c) 1988,1989,1990,1991,1992 by Richard Outerbridge.

[1] For each game session (every time the user inserts coins) the encryption key must remain the same as in the previous game session. This also means that the encryption key keeps unchanged for each encryption run. This gives us hints to the development of SpeedyDes3 to find a common pattern that can be used in all encryption procedures.

[2] SpeedyDes3 encryption was applied for a single block of 64 bits. The experimental results showed that SpeedyDes3 generally gains more than 1000 clock ticks in respect to the existing Des3 encryptions. In term of elapsed time on a standard PC the process of subkeys creation is about 28 times longer than the actual Des encryption.