Design and Implementation of Encrypted Card Reader

Kyi Kyi Khaing
Material Science and Material Engineering Research Center
Myanmar
akyitaw07@gmail.com

***Abstract*—The memory cards are widely used in several applications. This paper is intended to design and construct of the encrypted card reader. The basic building block in this design is the card reader, amplifier, multiplexer, and PC parallel port. This card can be used in license, passport, credit card, ID card, bank card, health care, travel and entertainment cards and etc. In this paper, data on a card can be protected against unauthorized viewing.**

Key words: Card Information; IR Sensors; IR Detectors; Multiplexer; Parallel Port; Optocoupler

I. Introduction

Card readers are simple devices that are very helpful for anyone who uses any type of card media. With all different devices using so many different types of memory cards it is a pain to have card readers for each different type of card. That is why card readers have become very popular. They can use many different types of memory cards. They are easy to use and travel with [9].

The card has emerged during the past decade as a remarkable technical solution to a variety of card system applications. Electronics cards have been developed for such traditional card uses as credit cards and banking applications as well as prepaid, throw-away cards, such as telephone cards. In addition, a great many novel applications have been propose which genuinely exploit the electric data processing available in the card [10].

II. Overview Of The System

The paper emphasizes on the encrypted data with the card and PC parallel port. The data based on the incoming card information. This data is used in this design. To simplify the hardware design, 5V power supply is decided to be used for the system. Thus, all components must be worked on 5V power supply. The card data and PC are used as the main of the system because the encrypted data stored in the card and PC.

A. Computerized Control Portion of the System

Among the I/O ports of the computer system, parallel interfacing is applied in this system to input the data and to output the display.

The standard parallel port uses three contiguous addresses, usually in one of these ranges:

3BCh, 3BDh, 3BEh
378h, 379h, 37Ah
278h, 279h, 27Ah

The first address in the range is the port's base address, also called the Data register or the port address. Among the Data pins of the parallel port, whose IO address is 0x378h, the D0 pin is used for select pin to the multiplexer. The second address is the port's Status register, the third is the Control register.

TABLE I. Data bits positioning in the Data Register

Pin	9	8	7	6	5	4	3	2
Data bits	8	7	6	5	4	3	2	1
0x378	D7	D6	D5	D4	D3	D2	D1	D0
System	-	-	-	-	-	-	-	Select

TABLE II. Status bits positioning in the Status Register

Pin	11	10	12	13	15	-	-	-
Status bits	8	7	6	5	4	3	2	1
0x379	$\overline{\text{BSY}}$	ACK	PAP	ON	ERR	-	-	-
System	Input	Input	Input	Input	-	-	-	-

TABLE III. Control bits positioning in the Control Register

Pin	-	-	-	-	17	16	14	1
Control bits	8	7	6	5	4	3	2	1
0x37A	-	-	-	-	$\overline{\text{DSL}}$	INI	$\overline{\text{ALF}}$	$\overline{\text{STB}}$
System	-	-	-	-	-	-	-	-

B. IR Sensing Portion of the System

IR diode use digital control signal that are modulated with a higher frequency carrier wave. The carrier wave; which is invisible to the human's eye. The digital control signals are relatively slow compared to the carrier frequency. The control pulse is sensed by infrared detector. Infrared detector requires the data signal to arrive in the form of a modulated signal. The modulation component is referred to as the carrier.

The detector internal circuitry consists of a bond-pass filter. The band-pass filter is to reject light energy or unwanted signals. The detector module increases the gain of the inter amplifier circuit. In bright lighting conditions, the internal gain is reduced. The effect of light levels is reduction of the overall operating distance of the IR LED and decreased IR detector module sensitivity.

C. Function Of Optocoupler

The primary function of an optocoupler or optoisolator is to provide electrical isolation between the devices connected to the transmitter (electrical circuit) and those connected to the receiver (PC). Information is transmitted through an optical link. If a computer, operated at 5V DC, were directly connected to circuitry controlling an electrical circuit, for example, the possibility would exist that a circuit failure could result in the high-voltage being applied directly to the computer [5].

Isolating the computer from the high-voltage circuit by using an optoisolator prevents the permanent damage that such a circuit failure could cause, since there is no physical connection between the transmitter and the receiver inside the optoisolator [6]. Fig. 1 shows the function of optocoupler.

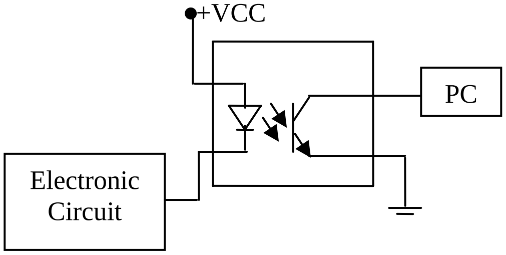


Figure 1. Function of Optocoupler

III. Hardware Implementation

A. Input Portion of the System

The coming data can be operated by the IR sensors according to the online demand and also can be operated manually. The output signals from the IR sensors are amplified by the transistor. The amplified signals output are connected to the 74LS157 input port to the parallel port. Fig. 2 shows input data to the parallel port.

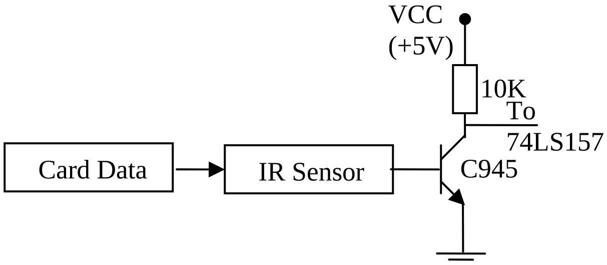


Figure 2. Input Data to the Parallel Port

B. Output Portion of the System

The parallel port uses one output and four inputs. One output is implemented with Data register (D0). Four inputs are implemented with Status registers (BSY, ACK, PAP and ON/OFF). The 74LS157 multiplexer IC uses four outputs and eight inputs. Four outputs are implemented with Pin 4, 7, 9 and 12. Eight inputs are implemented with Pin 2, 3, 5, 6, 10, 11, 13 and Pin 14. Output circuit diagram of 74LS157 is shown in Fig. 3.

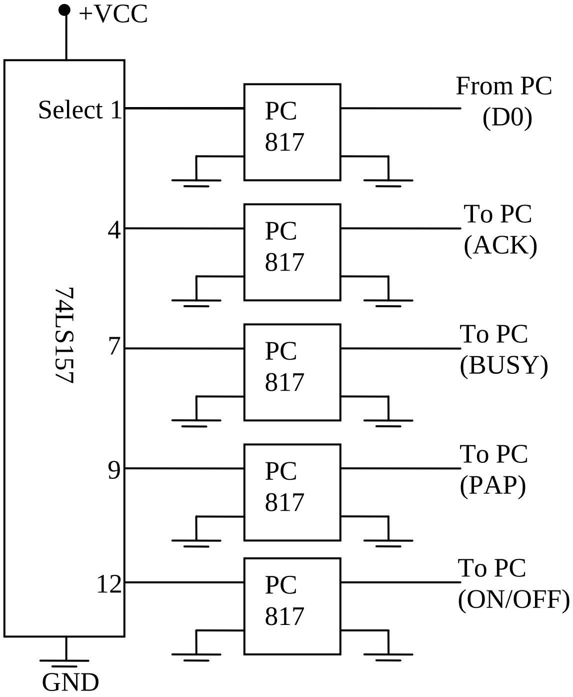


Figure 3. Output Circuit Diagram of 74LS157

C. Circuit Operation

The operation system of the encrypted card reader is as followed. In this circuit, the card information, IR sensors, 74LS157 multiplexer, PC817 (optocoupler) and PC parallel port are used. The block diagram of encrypted card reader is shown in Fig. 4.

When a card is inserted, the light coming into the sensor is focused on the detector elements by a fresher lens. The detectors are connected to oppose each other the sensor detects changes in infrared output signal. IR sensors sense the data and then, one side of the detectors are pulled up to 690 Ohm resistors.

The output signal is inserted to the base of the transistor. The small output voltage of the detector is amplified by the transistor (C945). The transistor is amplified from the output voltage of the IR sensors. After the voltage is amplified, the output signal is controlled by the select pin of the multiplexer. The select pin of multiplexer is controlled by the parallel port's output.

When the select pin is 1, the A inputs are selected. 1A passes through to 1Y; 2A passes through to 2Y etc. The Y outputs are connected up to the parallel port's status port; in such a manner that it represents the LSB (Least Significant Bit) 4 bits of the status register. First, the LSB 4 bits will be read. Then, the LSB 4 bits with data are transported to the PC.

Then, the select pin is 0, the B inputs are selected. The MSB (Most Significant Bit) 4 bits with data are transported to the PC. These '8' bits are alternate transported to the PC with interfacing PC817. PC817 is used to separate between the circuit and the Pc. The output 4 bits of multiplexer are inserted into the parallel port's input port. The data are taken from the PC with 4 bits during millisecond. In parallel port, data output pin is used the data select pin and the input 4 pins are used the coming data from the multiplexer.

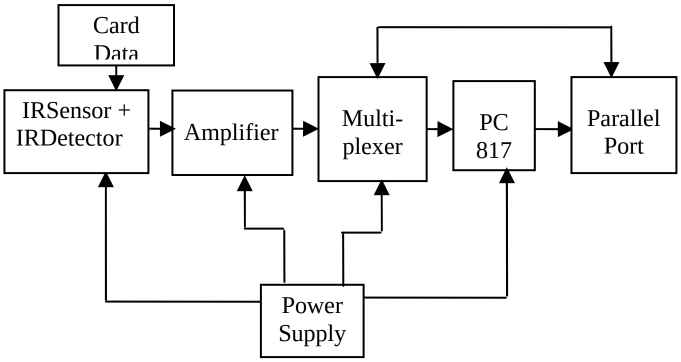


Figure 4. Block Diagram of Encrypted Card Reader

IV. Implementation of the Encrypted Card Reader

The encrypted card reader system is divided into two parts: card section and encrypted and decrypted program. The program encrypts the plain text file and decrypts the cipher text file. The user can use save the plain text file without encryption. Both conversion and encryption are written with Visual Basic codes. A VB script external functions call file are necessary for viewing and decrypting encrypted the file.

Maximum data can be used for encryption. The data used for encryption must be reused for decryption because the writer used single-key encryption. Conversion and encryption text file into encrypted file is shown in Fig. 5. Decryption and viewing encrypted text file into plain text file is shown in Fig. 6.

A. Encryption of Plain Text File

To encrypt the plain text message,

1. Open the message (plain text file) from a certain media
2. User can save the plain text message as text file without encryption
3. Convert and encrypt the plain text into encrypt text file using the data
4. The text file is changed to encrypt text file

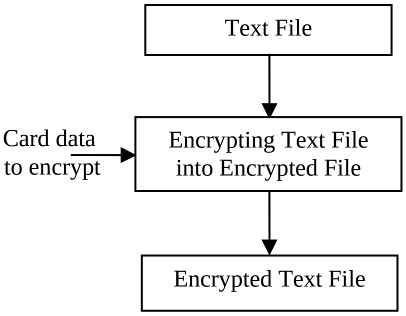
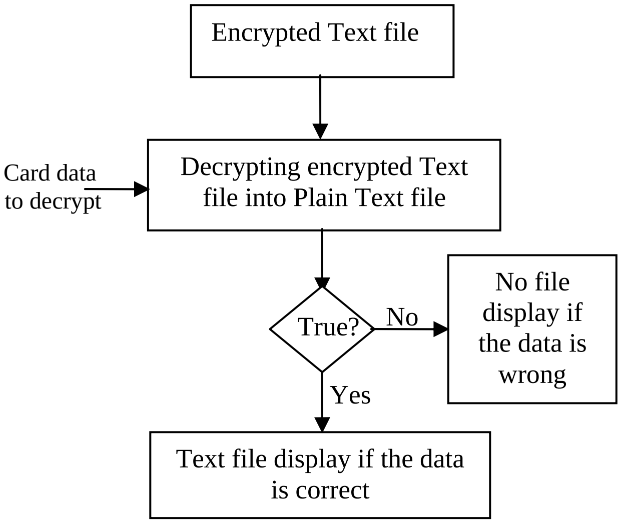


Figure 5. Conversion and Encryption Text file into Encrypted File

B. Decryption Of Encrypted Text File

To decrypt the encrypted text file

1. The text file is opened from menu
2. The text file with decrypt button will appear on the screen
3. Decrypt the text file using the data which has used in encryption
4. If the data is correct, the page will appear, otherwise the page will not appear correctly



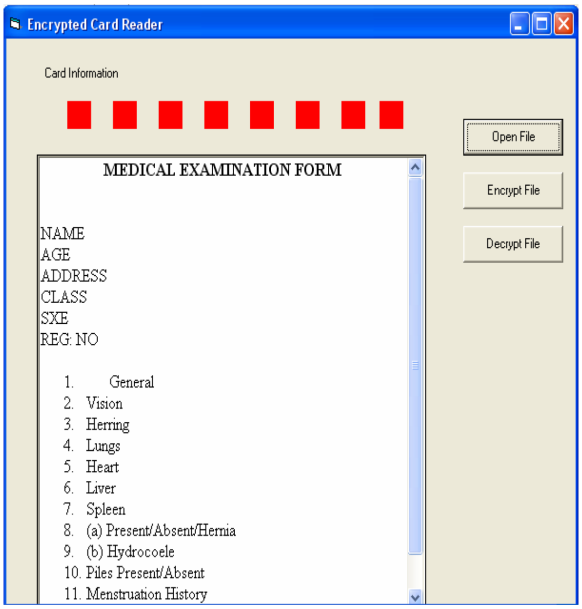
Encrypted Text file
Card data to decrypt
Decrypting encrypted Text file into Plain Text file
True?
No
No file display if the data is wrong
Yes
Text file display if the data is correct

Figure 6. Decryption and Viewing Encrypted Text File into Plain Text File

C. Software Implementation

In this program, it shows text file such as plain text and cipher text in the host system and in the card information. If open file button is clicked, open file dialog box will appear.

In the dialog box, the file to be viewed must be chosen. After the file has been chosen, it will be shown in Rich Text Box. Encrypted card reader dialog box can be used. It contains Open file, Encrypt file and Decrypt item. Encrypt item encrypt user information file in the host system and Decrypt item deciphers the cipher text file in the card information.



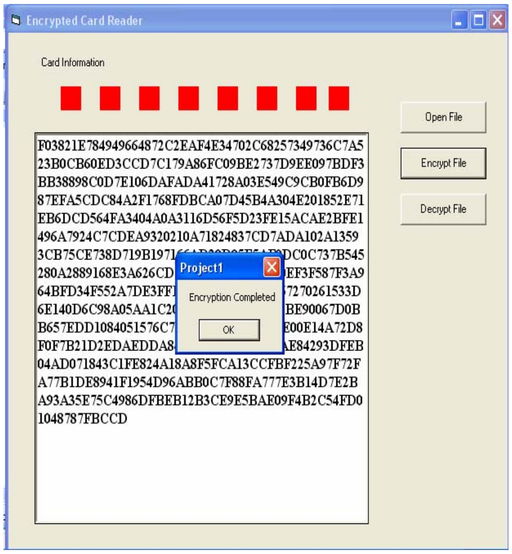
MEDICAL EXAMINATION FORM

NAME
AGE
ADDRESS
CLASS
SXE
REG: NO

1. General
2. Vision
3. Herring
4. Lungs
5. Heart
6. Liver
7. Spleen
8. (a) Present/Absent/Hernia
9. (b) Hydrocoele
10. Piles Present/Absent
11. Menstruation History

Figure 7. Encrypted Card Reader's Card Information

If Open file is clicked, Fig. 7 shows encrypted card reader's card information. Then, the user must type plain text file name to encrypt, one key and cipher text file name to save the encrypted data in the card. Fig. 8 shows the encryption completed diagram.



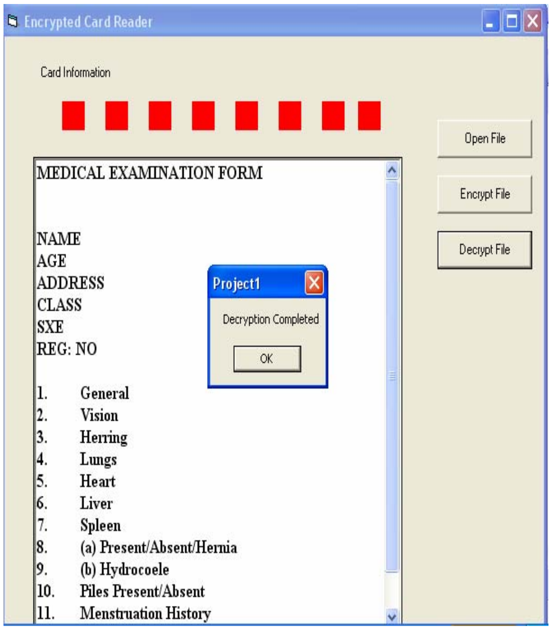
```
F03821E784949664872C2EAF4E34702C68257349736C7A5
23B0CB60ED3CCD7C179A86FC09BE2737D9EE097BDF3
BB38898C0D7E106DAFADA41728A03E549C9CB0FB6D9
87EFA5CDC84A2F1768FDBCA07D45B4A304E201852E71
EB6DCD564FA3404A0A3116D56F5D23FE15ACAE2BFE1
496A7924C7CDEA9320210A71824837CD7ADA102A1359
3CB75CE738D719B1971                    DC0C737B545
280A2889168E3A626CD                    EF3F587F3A9
64BFD34F552A7DE3FF                     7270261533D
6E140D6C98A05AA1C2                     BE90067D0B
B657EDD1084051576C7                    E00E14A72D8
F0F7B21D2EDAEDDA8                      AE84293DFEB
04AD071843C1FE824A18A8F5FCA13CCFBF225A97F72F
A77B1DE8941F1954D96ABB0C7F88FA777E3B14D7E2B
A93A35E75C4986DFBEB12B3CE9E5BAE09F4B2C54FD0
1048787FBCCD
```

Encryption Completed

Figure 8. Encryption Completed Diagram

Then, the user must type cipher text file name to decrypt, one key and plain text file name to save the decrypted data in the card. Fig. 9 shows the decryption completed diagram.

And then, the user must type cipher text file name to decrypt, if other key is used in decryption, the file will not open the original data. The decrypted data is shown in the host system. The decryption diagram can be seen in Fig. 10.



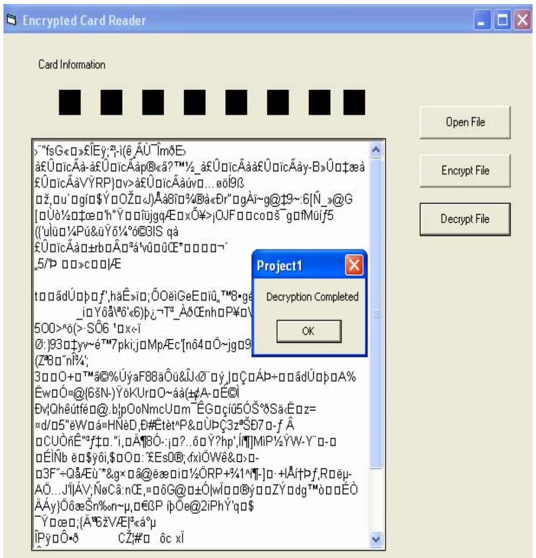
MEDICAL EXAMINATION FORM

NAME
AGE
ADDRESS
CLASS
SXE
REG: NO

Decryption Completed

1. General
2. Vision
3. Herring
4. Lungs
5. Heart
6. Liver
7. Spleen
8. (a) Present/Absent/Hernia
9. (b) Hydrocoele
10. Piles Present/Absent
11. Menstruation History

Figure 9. Decryption Completed Diagram



```
›¨"fsG«□»£ÎEÿ;²¦-ì(ê¸ÃÙ¯ÎmðE›
à£Û□ïcÃà-à£Û□ïcÃàp®«ã?™½_à£Û□ïcÃàà£Û□ïcÃày-B»Û□‡æà
£Û□ïcÃàVŸRP}□v>à£Û□ïcÃàúv□…øöÍ9ß
□ž,□u´□gí□$Ý□OŽ□‹J)Åà8î□¾®à«Ðr"□gÀï~g@‡9~:6[Ñ_»@G
[□Ùò½□‡œ□'h"Ÿ□□ïüjgqÆ□xÕ¥>¡OJF□□co□š¯g□fMüíƒ5
({'uÌü□¼Pú&üŸõ¼°ó©3IS qà
£Û□ïcÃà□±rb□Â□³á¹vû□ûŒ*□□□□¬´
„5/'Þ □□»c□□|Æ

t□□ãdÚ□þ□ƒ',häÊ»ï□;ÕOëìGeE□ïû„™8•gé
        _i□Yôå\ªô'«6)þ¿¬T³_ÀðŒnh□P¥□V
5O0>^ö(>·SÔ6 ¹□x‹ï
Ø:}93□‡yv~é™7pki;j□MpÆc'[nô4□Ö~jg□9
(Zª8□˝nÎ³¼';
3□□O+□™ã©%ÚýaF88äÔü&ÎJ‹Ø¨□ý¸|□Ç□ÁÞ÷□□ãdÚ□þ□A%
Ëw□Ó⁎@{6šN-)ŸöKUr□O~áà(±¢A-□É©Ì
Ðv¦Qhêútfé□@.b¦pOoNmcU□m¯ÊG□çíû5ÓŠ°ðSä‹Ë□z=
⁎d/□5"ëW□á⁎HÑèD,Ð#Ëtèt^P&□ÙÞÇ3zªŠÐ7□-ƒ Â
□CUÒñÊ"³ƒ‡□."i,□Ä¶8Ó-:¡□?..õ□Ÿ?hp',Íí¶]MiP½ŸW-Y¨□-□
□ÉÌÑb ë□$ÿôì,$□O□:˜£Es0®;‹fxìÖWê&□›□-
□3F˝÷QåÆù´*&g×□â@ëæ□i□½ÖRP+¾1^í¶-]□·+lÅí†Þƒ,R□ëµ-
AÖ…J'Ï|ÁV;ÑøCâ:nŒ,⁎□ôG@□±Ó|wÏ□□®ý□□ZÝ□dg™ò□□ÉÒ
ÄÁy}ÖôæŠn‰n~µ,□€ßP íþÖe@2iPhÝ'q□$
¯Ÿ□œ□;{Ä¶6žVÆ|³«á°µ
ÎPÿ□Ô•ð        CŽ¦#'□   ôc xÏ
```

Decryption Completed

Figure 10. Decryption Diagram

D. Summary

In this paper, the implementation of the card system is described. Flowchart and block diagram are mentioned. The card system has been developed for the security of patient data. It can construct encrypt and decrypt the medical records. Moreover, it can be used to save user's important data with strong security. So, card system will remain in main role at security today, tomorrow and next. Today World is meeting with problem of security.

Therefore, this system will help these problems with the crypto-system.

V. CONCLUSION

A card, that is used for the medical record, passport, driving license, credit and debit card and access to the place of work will undoubtedly alter human relationships due to its potential uneasiness of what data is held, accessed and modified. Such cards are already being piloted.

Some of the potential benefits of cards are:

- Using cards is safer than carrying cash for an individual
- Cards can improve access to services for the disable and elderly
- It is a secure means of authenticating the identity of reader device. It is a portable and secure store of information available to all
- Access can be made available in geographical locations where on-line communication is not possible. So, the opportunity of fraud I reduced by using cards.

Therefore, cards offer great potential benefits to society.

ACKNOWLEDGMENT

I also acknowledge all my friends who helped towards the successful completion of this paper. My special thanks are due to all my teachers who taught me and gave their knowledge to me. Special thanks are also extended to all those who where directly or indirectly involved towards the successful completion of this paper.

REFERENCES

[1] DAVID CHAUM, "Selected papers from the second international Smart Card 2000 conference" Amsterdam, Netherlands, 4-6 October 1989.

[2] Glass, A.S. & Massey, J.L, 1985; "Plastic Card"

[3] J.Webb, K.Greshock, "Industrial Control Electronics", Merrill Publishing Company, 1990.

[4] Karadigudda, M. 1997, Smart Cards, Department of Computer Science, San Jose State University, 2006.

[5] Optocouplers: "When and how to use them," Electus Distribution Reference Datasheet.

[6] R.M. Marston, Optoelectronics Circuits Manual, 2nd Ed, Newnes, 1999.

[7] T.E. Kissell, "Industrial Electronics", Prentice Hall International, Inc, 1997.

[8] Thomas L.Flovd, "Electronics Device", 5th Edition.

[9] "Introduction of Card". http://www/smartid.gov.hk/en/reader/index.html.

[10] "Card Reader", http://www.thinkcomputers.org/index.php.

[11] "Data Encryption and Data Decryption" http://www.msdn2.microsoft.com/en.us/library

[12] "Data Encryption Standard" http://www.en.wikipedia.org/wiki/ Data- Encryption-Standard