

Encryption

Table of Contents

- [DES - Data Encryption Standard](#)
- [NBS - National Bureau of Standards](#)
- [FIPS - Federal Information Processing Standards](#)
- [NTIS - National Technical Information Service](#)
 - [Information on the NTIS database](#)
 - [Other References](#)

Encryption

Blue Cross and Blue Shield of Alabama has decided to use Data Encryption Standard (DES) as the encryption method for the InfoSolutions Medical Information Network. DES operates in several modes and we have chosen cipher-block-feedback (CFB) as the mode for data encryption. The key used as input to the DES routine is generated as follows:

The keystring is padded with blank characters to a positive multiple of eight. A secondary key is generated from the first eight characters of the keystring by shifting each character left by one bit (discarding each 8th-order bit). This 64-bit authentication code is the encryption key. This is the same method used by Federal Information Processing Standards (FIPS) publication 112 except the authentication code is not converted into printable form. This is also identical to FIPS publication 113 with the input padded with blanks instead of zeros.

Below is a short description of DES and references to material, which can be used to aid in implementing DES encryption.

Encryption will be required on all Patient Medical transactions. Once you begin using encryption for a provider, all transactions for that provider must be encrypted. The provider's password will be used as the key for encryption / decryption and the provider must have the ability to modify his password.

Once the transaction has been encrypted, the result must be treated as a binary file. This means that the file cannot be read and written as byte characters without unpredictable results. In order to alleviate this problem, we will be using the uuencode and uudecode utilities to convert the binary file to a string of characters, and vice versa, for transmission purposes. The uuencode and uudecode utilities are part of the Unix environment; however, versions are available for other platforms. Please contact Blue Cross and Blue Shield of Alabama if you need assistance in this area.

DES - Data Encryption Standard

The National Bureau of Standard's (NBS) popular, standard encryption algorithm. It is a product cipher that operates on 64-bit blocks of data, using a 56-bit key. It is defined in FIPS 46-1 (1988) (which supersedes FIPS 46 (1977)). DES is identical to the American National Standards Institute (ANSI) standard Data Encryption Algorithm (DEA) defined in ANSI X3.92-1981.

NBS - National Bureau of Standards

National Bureau of Standards: part of the US Department of Commerce, now the National Institute of Standards and Technology (NIST).

FIPS - Federal Information Processing Standards

Federal Information Processing Standards

United States Government technical standards published by the National Technical Information Service (NTIS). Computer-related products bought by the US Government must conform to these standards.

NTIS - National Technical Information Service

National Technical Information Service

Information on the NTIS database

This information is available as reports, videos, software, and data files and represents hundreds of billions of dollars of research sponsored by U.S. and foreign governments.

If you have a personal computer, there are two ways to digitally access the NTIS Bibliographic Database: On-line or by using CD-ROM. If you do not have a personal computer, check either your company library or a public or academic library; most already have access to the database.

Several on-line services allow you to connect to the database by modem. If you expect to become a heavy user of the database, you might also want to consider purchasing the database on CD-ROM.

If you're unfamiliar with how to search the database or would like on-line or CD-ROM training, NTIS offers trained staff to help you.

The commercial services listed below provide on-line access to the NTIS Database. Call them for more information on getting started.

The NTIS Bibliographic Database is available from:

CDP Technologies, (800) 950-2035;

CISTI, in Canada, (613) 993-1210;

DATA-STAR, (800) 221-7754;

DIALOG, (800) 334-2564;

ESA/IRS in Italy, Fax 39/6 94180361;

KNOWLEDGE EXPRESS, (800) 248-2469;

ORBIT/QUESTEL, (800) 456-7248, in Virginia, (703) 442-0900; and

STN International, (800) 848-6533, in Ohio and Canada (800) 848-6538.

Purchasing your own CD-ROM copy of the database gives you a flat-fee, unlimited-use opportunity to review NTIS records with abstracts. To use the NTIS CD-ROM, you need a personal computer equipped with a CD-ROM reader.

Two companies offer the database on CD-ROM; DIALOG Information Services and SilverPlatter Information Service, Inc. Local area network options are available through both companies, and both services update the CD-ROM quarterly.

DIALOG's CD-ROM version of the database includes records from 1980 to the present. SilverPlatter's CD-ROM version of the database includes records from 1983 to the present.

For more information, contact: DIALOG, (800) 334-2564 or SilverPlatter, (800) 343-0064.

Other References

Books with DES Source Code

"Applied Cryptography", Bruce Schneier, John Wiley & Sons, ISBN 0-471-59756-2 (C).

"The Standard Data Encryption Algorithm", Harry Katzan Jr., Petrocelli Books, 1977 ISBN 0-89433-016-0 (APL).

"Computer Networks", Andrew S. Tanenbaum, Prentice Hall (both editions; second edition is ISBN 0-13-162959-X0). (Pascal).

"Numerical Recipes", William H. Press et al, Cambridge University Press. (Fortran and Pascal version is ISBN 0-521-30811-9. Also in "Numerical Recipes in C").

"UNIX System Security", Wood and Kachan, Hayden. ISBN 0-8104-6267-2.

Byte Magazine, April 1977 (6502 Assembler).

"Cryptography: An Introduction to Computer Security", Seberry and Pieprzyk, Prentice Hall Australia. (c).

"Mathematical Cryptology for Computer Scientists and Mathematicians", Wayne Patterson, Rowman and Littlefield, 1987. ISBN 0-8476-7438-X.

Introduction to the Analysis of the Data Encryption Standard (DES), by Wayne G. Barker, ISBN 0-89412-169-3 (soft cover), 0-8412-170-7 (library bound), 1991, Agean Park Press, Appendix G. (Basic of all things).