History Of The Data Encryption Standard (DES)

Based on *Applied Cryptography* by Schneier, Chapter 12

Lecture notes of Alexander Wood
awood@jjay.cuny.edu

John Jay College of Criminal Justice

The DES

The **Data Encryption Standard (DES)** is a private-key algorithm for encryption. It was developed in the 1970s and remained a worldwide standard for over 20 years after its publication.

Early 1970s: Haphazard Cryptography

Back in the early 1970s, the NSA was not even admitting their existence. The military had their own private communication methods, and several companies sold cryptographic equipment – but the encryption methods were not public.

Kerckhoff's Principle

Recall Kerckhoff's Principle, which states that *the details of the cryptosystem should be able to be shared publicly* without compromising security.

However, details about the commercial encryption methods at the time were not available.

The Search For An Encryption Standard

Once upon a time there was no good way for outside secret agencies to judge good crypto
EBG13 is good
Double ROT13 is better
A decree went throughout the land to find a good secure algorithm
WE NEED A GOOD CIPHER !

Image from: `https://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/`

The Search for an Encryption Standard

DEPARTMENT OF COMMERCE ★ NATIONAL BUREAU OF STANDARDS ★

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

1972: The National Bureau of Standards, now called the **National Institute for Standards and Technology (NIST)**, requested proposals for a cryptographic algorithm which could be put to standard use by the public.

NIST's Design Criteria

NIST provided the following design criteria:

- The algorithm must provide a high level of security.
- The algorithm must be **completely specified** and easy to understand.
- The **security of the algorithm must reside in the key**; the security should not depend on the secrecy of the algorithm. ← ***Kerckhoff's Principle!!!!***
- The algorithm must be **available to all users**.
- The algorithm must be adaptable for use in diverse applications.
- The algorithm must be economically implementable in electronic devices.
- The algorithm must be **efficient** to use.
- The algorithm must be **able to be validated**.
- The algorithm must be exportable.

Cryptographic Standard: The Search Is On!

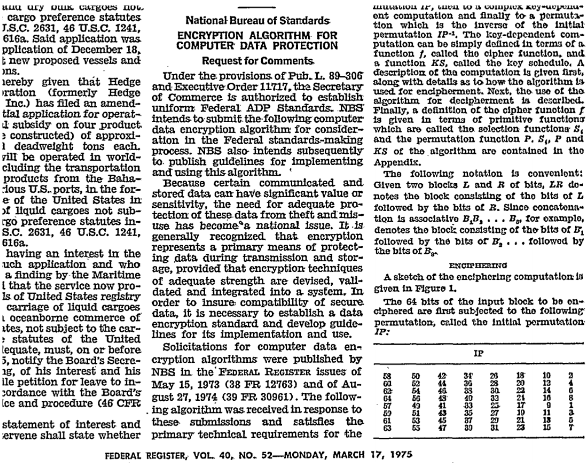
Many ideas were proposed, but it took a while to find one which truly satisfied security requirements.

The Search Ends With... Lucifer

During the early 1970's, researchers at IBM created a symmetric-key cipher called **Lucifer**, now known as the **Feistel cipher**.

Horst Feistel

Publication of the DES



and dry bulk cargoes not
cargo preference statutes
J.S.C. 2631, 46 U.S.C. 1241,
616a. Said application was
pplication of December 18,
t new proposed vessels and
ons.
hereby given that Hedge
oration (formerly Hedge
Inc.) has filed an amend-
tial application for operat-
d subsidy on four product
e constructed) of approxi-
l deadweight tons each.
will be operated in world-
cluding the transportation
products from the Baha-
rious U.S. ports, in the for-
e of the United States in
of liquid cargoes not sub-
rgo preference statutes in-
S.C. 2631, 46 U.S.C. 1241,
616a.
having an interest in the
uch application and who
a finding by the Maritime
l that the service now pro-
ls of United States registry
carriage of liquid cargoes
ı oceanborne commerce of
ates, not subject to the car-
e statutes of the United
lequate, must, on or before
5, notify the Board's Secre-
ng, of his interest and his
ile petition for leave to in-
cordance with the Board's
ice and procedure (46 CFR

statement of interest and
ervene shall state whether

National Bureau of Standards

ENCRYPTION ALGORITHM FOR COMPUTER DATA PROTECTION

Request for Comments

Under the provisions of Pub. L. 89–306 and Executive Order 11717, the Secretary of Commerce is authorized to establish uniform Federal ADP Standards. NBS intends to submit the following computer data encryption algorithm for consideration in the Federal standards-making process. NBS also intends subsequently to publish guidelines for implementing and using this algorithm.

Because certain communicated and stored data can have significant value or sensitivity, the need for adequate protection of these data from theft and misuse has become a national issue. It is generally recognized that encryption represents a primary means of protecting data during transmission and storage, provided that encryption techniques of adequate strength are devised, validated and integrated into a system. In order to insure compatibility of secure data, it is necessary to establish a data encryption standard and develop guidelines for its implementation and use.

Solicitations for computer data encryption algorithms were published by NBS in the FEDERAL REGISTER issues of May 15, 1973 (38 FR 12763) and of August 27, 1974 (39 FR 30961). The following algorithm was received in response to these submissions and satisfies the primary technical requirements for the

mutation *IP*, then to a complex key-dependent computation and finally to a permutation which is the inverse of the initial permutation IP^{-1}. The key-dependent computation can be simply defined in terms of a function *f*, called the cipher function, and a function *KS*, called the key schedule. A description of the computation is given first, along with details as to how the algorithm is used for encipherment. Next, the use of the algorithm for decipherment is described. Finally, a definition of the cipher function *f* is given in terms of primitive functions which are called the selection functions S_i and the permutation function *P*. S_i, *P* and *KS* of the algorithm are contained in the Appendix.

The following notation is convenient: Given two blocks *L* and *R* of bits, *LR* denotes the block consisting of the bits of *L* followed by the bits of *R*. Since concatenation is associative $B_1B_2 \ldots B_8$, for example, denotes the block consisting of the bits of B_1 followed by the bits of $B_2 \ldots$ followed by the bits of B_8.

ENCIPHERING

A sketch of the enciphering computation is given in Figure 1.

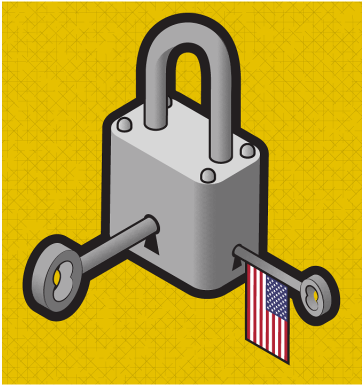
The 64 bits of the input block to be enciphered are first subjected to the following permutation, called the initial permutation *IP*:

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

FEDERAL REGISTER, VOL. 40, NO. 52—MONDAY, MARCH 17, 1975

NIST, IBM, and the NSA teamed up to evaluate the algorithm's security and suitability. Eventually in 1975 a modifed version of the algorithm was published in the *Federal Register* on March 17, 1975.

Backdoor Controversy



http://www.vocativ.com/297409/presidential-candidate-encryption/

People were concerned that the NSA had included a “backdoor” in the DES.

A **backdoor** secret method by which a cryptographic system can be bypassed in order to obtain access to the plaintext of an encrypted message.

Discussions about government backdoors and surveillance are increasingly relevant with current-day encryption.

Backdoor Controversy: Key Length

The controversy was rooted in the fact that the key length used in DES is only 56 bits.

Even before the DES was officially adopted as a standard, many asserted that this key length was too short – and suspected that it had purposely been designed that way by the NSA.

1977: Diffie and Hellman's Brute-Force Attack

Merkle, Diffie, and Hellman in 1977

Diffie and Hellman proposed a $20 million dollar machine in 1977 which would be able to recover a DES key in one day. It exploited the small key length used by DES.

1993: Wiener's Brute-Force Attack

In 1993, Michael Wiener designed a machine exploiting the short key length which, when built with 5760 chips, could be made for $100K and find a DES key in 1.5 days. When built with 57600 chips the cost would be $1 million but the DES key could be recovered in 3.5 hours.

Neither Diffie and Hellman's machine nor Wiener's machine are known to have been made, but they showed that the DES could potentially be comprimised by even a brute-force attack.

1976: Adoption As Federal Standard

DEPARTMENT OF COMMERCE ★ UNITED STATES OF AMERICA ★

The DES was adopted as a Federal Information Processing Standard (FIPS) on November 23, 1976 by the Secretary of Commerce. The official description of the standard was published in 1977. The DES was authorized for use for unclassified government communications.

The NSA's Regrets

The DES was the first NSA-evaluated algorithm to be made public. It is speculated that this was on accident – the NSA believed the DES was hardware-only and did not realize that NIST would publish enough information for the public to develop their own cryptographically secure software.

The NSA claims off the record that publishing the DES was one of their biggest mistakes. Future algorithms remained classified.

1981: Adoption as a Private-Sector Standard

ANSI American National Standards Institute

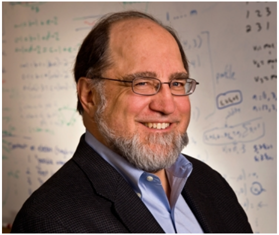
In 1981 the American National Standards Institute (ANSI) approved DES as a standard in the private sector and published their own standard for modes of operation. Within ANSI, groups represented retail and banking developed their own standards based off of DES.

1992-1998: Time Marches On

There was still not an alternative to the DES in 1992. It was recertified by NIST to remain the standard until 1998, and in 1997 a formal request was issued to search for alternatives during those years – as it was suspected that the “lifetime” of the DES would end by the late 1990s.

Rivest's Contests

Ronald Rivest (the 'R' of 'RSA') funded four contests to break a DES encrypted message.



Ronald Rivest

- (Contest 1) 1996, broken in 96 days using distributed networks
- (Contest 2) 1997, broken in 41 days
- (Contest 3) 1998, broken in 56 hours using the Deep Crack computer
- (Contest 4) 1999, broken in 22 hours 15 minutes using Distributed Net and the EFF machine

2001: Selection of AES Algorithm

After announcing their intention to find a successor for DES in 1997, NIST selected an algorithm designed by Belgian cryptographers Joan Daemen and Vincent Rijmen called **Rijndael**.

This cipher was modified and re-named the **Advanced Encryption Standard (AES)**, the chosen successor to DES.

2005: DES Officially Withdrawn

The DES was officially withdrawn in 2005. Triple DES, or **3DES**, is approved for sensitive government communication through 2030.

3DES applies three iterations of DES which increases the key length to 168 bits. Meet-in-the-middle attacks reduce the level of effective security which 3DES can offer to 112 bits.

The Legacy of DES

The DES has reached the end of its useful lifetime. However, the DES was the first cryptosystem of its caliber to have its algorithms made public.

This revitalized the academic study of cryptography and spurred the development of modern cryptography as it is known today.

References

- *Applied Cryptography* By Schneier, Chapter 12
- https://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
- http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard
- http://www-math.ucdenver.edu/~wcherowi/courses/m5410/des.pdf