

# The Enduring Value of Symmetric Encryption

## White Paper

August 2000

[www.eAladdin.com](http://www.eAladdin.com)

This paper may be distributed freely provided that its content is not modified, that it is distributed in its entirety, and that all trademark notices are left intact.

eToken is a trademark or registered trademark of Aladdin Knowledge Systems, Inc.

Microsoft and Windows are trademarks of Microsoft Corporation.

All other product names mentioned herein are trademarks of their respective owners.

## Table of Contents

The Enduring Value of Symmetric Encryption.....	5
Encryption Overview .....	5
Comparison and Conclusions .....	5
Advances in Encryption Technology.....	6
Encryption Technology Research.....	6
Encryption Methods.....	7
Symmetric Encryption .....	7
Asymmetric Encryption .....	7
Comparison of Methods .....	7
Method Comparison Summary.....	8
Authentication Applications .....	9
Symmetric Authentication .....	9
Asymmetric Authentication.....	9
Key Database Management.....	9
Mutual Authentication.....	9
Authentication Security and Efficiency.....	9
Authenticated Key Exchange .....	10
Disk Encryption .....	11
Symmetric Smart Cards and Tokens.....	11
Choosing the Right Symmetric Key Algorithm .....	11
Alternatives to the DES Algorithm .....	12
Encryption and eToken Functionality .....	12
Encryption Application Summary.....	13
Summary of Conclusions.....	14
References.....	15

## **Acknowledgements**

Aladdin Knowledge Systems Ltd acknowledges the contribution of Yehuda Lindell, of the Weizmann Institute of Science in Israel, in the preparation of this paper (see reference [L] on page 15).

As we move forward in the digital era, we are constantly faced with challenges presented by an information flow that is more volatile than ever before, inherently less secure, and often stripped of its integrity.

The success of e-commerce and enterprise security depends essentially on the ability to control data access and to protect private and proprietary information. In this context, we can understand the paramount importance of the invention, development and appropriate use of highly sophisticated encryption methods.

### Encryption Overview

Encryption refers to the translation of data into an encoded format for the purpose of achieving data security. Reading an encrypted file requires access to a secret key, which enables the decryption of this file.

The two primary encryption methods in existence today are:

- **Symmetric encryption**, also known as secret key cryptography, which requires the sender and receiver of a message to share the use of a single, common key for encryption and decryption.
- **Asymmetric encryption**, also known as public key cryptography, which employs two keys: a public key to encrypt messages and a private key to decrypt them.

Asymmetric encryption is currently viewed as the security technology of the future, making it the focus of most of today's security development efforts. However, symmetric encryption continues to offer significant benefits and is still suitable for many security applications.

### Comparison and Conclusions

This paper compares the functionality, benefits and suitability of symmetric and asymmetric encryption methodology, and presents the following conclusions:

- While asymmetric encryption provides undeniable advantages in terms of functionality, there are many applications for which symmetric encryption is the best choice, providing high security that is both efficient and most cost-effective.
- Applications such as laptop access security, or remote authentication for restricted websites, do not require full asymmetric smart card technology. Symmetric USB tokens provide the high security that these applications need, at significantly lower cost.

## **Advances in Encryption Technology**

As technology moves forward, so do the advances in public key security methods such as asymmetric encryption. To promote the use of products and services based on Public Key Infrastructure (PKI), an international organization has been formed, known as the PKI Forum. In addition to its work with PKI, this non-profit, multi-vendor organization promotes the value of asymmetric encryption technology in e-commerce applications.

As a security solutions provider and active participant in the PKI Forum, the development team at **Aladdin Knowledge Systems** researches and introduces innovations in the field of information security and cryptography. Recently, Aladdin introduced *eToken R2*, the world's first USB-based token device to integrate DESX algorithm encryption technology.

For a more detailed description of the *eToken R2*, visit the Aladdin Security Portal at [www.eAladdin.com](http://www.eAladdin.com).

### **Encryption Technology Research**

The work of the Aladdin R&D team draws from research work at various centers of excellence, including research being conducted at the Weizmann Institute of Science in Israel, and input from the notable security expert Philip Rogaway (see references [L] and [KR] on page 15).

As Aladdin explores and introduces innovations in encryption technology, it also explores the synthesis of existing technology with state-of-the-art developments to maximize security options.

With help from multiple sources, Aladdin has conducted extensive research, resulting in the conclusion that symmetric key technology provides significant reasons for inclusion as an important encryption-based security solution. The sections that follow describe these reasons in greater detail.

This section describes and compares the principal aspects of the symmetric and asymmetric encryption methods in greater detail.

When organizations are faced with a choice of security options, the most frequently chosen security mechanism is the one that addresses the highest level of security required at the lowest cost. With the wide range of security options on offer, organizations can select the most appropriate security solution for the task.

### Symmetric Encryption

Symmetric cryptography involves two parties who share a joint secret or key. This exclusive knowledge of the key enables private and secure communication between the two parties, without the threat of a third party eavesdropping or otherwise tampering with messages in transit. In this instance, the same key is used for encryption and decryption.

We will use the classic pseudonyms, Alice and Bob, to represent the two parties. In the symmetric cryptography model, both Alice and Bob, and only Alice and Bob, must have access to the same key.

While symmetric encryption is ideal for many applications, the need to exchange keys and to maintain a direct relationship between the two parties makes this type of encryption unsuitable for e-commerce on a commercial scale.

### Asymmetric Encryption

The development of asymmetric encryption, based on public key technology, ushered in the age of modern cryptography. This method employs a pair of keys, consisting of a public key and a private key.

Alice can publicize her public key so that anyone who wants to send her an encrypted message can do so. However, only Alice can decrypt the message using her private key. Thus, the ability to encrypt a message is extended to the public, while the ability to decrypt the message is securely retained by the owner of the private key.

The algorithms used in asymmetric encryption, such as RSA, are usually based on solving number-theoretic problems. The security of these algorithms is assured by the inherent difficulty of solving such problems, for example, decomposing large numbers into their prime factors. The knowledge of these prime factors, incorporated into Alice's private key, enables her to execute a task that no one else can, for example, decrypting a message encrypted with the public key.

Such asymmetric encryption techniques form the backbone of modern e-commerce.

Examples of e-commerce applications made possible using asymmetric encryption and PKI include:

- The verification and non-repudiation of a customer's digital signature on an electronic transaction.
- The establishment of a secure communication line for electronic transactions without the prior requirement to exchange keys or secrets. This is crucial for B2C transactions.

The e-commerce world is currently promoting asymmetric encryption as the solution to all our security needs. Many have all but abandoned symmetric keys, except as a supporting tool for use in protocols based on asymmetric public key technology.

### Comparison of Methods

Although asymmetric encryption provides far more functionality, there are still many applications in which symmetric encryption is the best solution, and does the job as

securely and more efficiently. Due to its nature, symmetric technology is far less expensive to implement.

The principal aspects of the two methods are compared below:

	<b>Symmetric Encryption</b>	<b>Asymmetric Encryption</b>
<b>Functionality</b>	Allows efficient communication between two parties in a closed environment.	Enables security in settings in which symmetric encryption simply does not work or is more difficult to implement.
<b>Computational efficiency</b>	Computes incredibly fast, since the relatively simple operations used are executed very efficiently.	Computes slowly, using computationally heavy and complex operations, based on the difficulty of solving number-theoretic problems.
<b>Key size</b>	Uses 128-bit symmetric keys, which are considered very secure.	Employs key sizes of at least 1000 bits to achieve sufficient, lasting security.
<b>Hardware</b>	Performs simple algorithms, requiring relatively inexpensive hardware.	Implements complex and time-consuming algorithms that need more powerful hardware.
<b>Security</b>	No difference. Security is based on the strength of the algorithm and size of the key. Good algorithms exist for both encryption methods. Key size effectiveness, as shown above, is dependent on the encryption method.	

### Method Comparison Summary

The advantage of asymmetric encryption is in its functionality. It provides security in a wide range of applications that cannot be solved using only symmetric techniques. However, we pay a price for this in computational efficiency and increased cost.

There is no difference between the encryption methods with regard to security. For applications in which either symmetric or asymmetric encryption is suitable, a claim that one type of encryption is more secure than the other is false and misleading.

In many settings, the efficiency hurdle can be overcome by combining both methodologies, as in the following example:

- A message is encrypted with a symmetric key, which is chosen and used for this transaction only.
- This symmetric key is encrypted with the recipient's public key.
- Both the encrypted message and the encrypted key are sent to the recipient, who decrypts the symmetric key with his private key, and then uses it to decrypt the message.

This method combines the efficiency of symmetric encryption with the advantages of an asymmetric setting.

This section describes and compares the two encryption methods in relation to authentication applications, and outlines the issues connected with authentication.

Authentication is used in many settings that require users to prove their identity. For example, when users log in to a PC, local network or remote server, or when accessing a restricted website, their identity and access permissions must be authenticated, using symmetric and/or asymmetric authentication techniques.

### Symmetric Authentication

With symmetric authentication, the user and the server both share a secret key. The ability to encrypt a random message proves knowledge of the key.

An authentication protocol is based on the server sending a random challenge and the user returning the encrypted value. The server then encrypts the challenge with the user's key and compares the results.

Using a random message guarantees that:

- The challenge is different each time it is issued.
- It is impossible to guess what the challenge may be in the future.
- Identification is confirmed only if the correct user's key is present at the exact moment of authentication.

### Asymmetric Authentication

With asymmetric authentication, the user's private key provides access to the secret identifying information and acts as a signing key. The user's public verification key is stored on the server. Identification is confirmed when the user signs on a random string sent by the server, using the appropriate private key.

### Key Database Management

With symmetric encryption, the server must maintain a database of user identities and their secret keys. Due to the fact that knowledge of a key enables impersonation, the database containing users' identities and their keys must be kept secure.

In order to verify the signatures used for authentication with asymmetric encryption, the server must maintain a database of user identities and their associated public verification keys. An important advantage of asymmetric key management is that the database need not be kept secret. However, it must be secure from external tampering to prevent attackers from changing the public key associated with a given user to one for which the private key is known.

### Mutual Authentication

Symmetric encryption enables mutual authentication at no extra cost or overhead. Asymmetric encryption requires the user to have the public verification key of the server.

In a mutual authentication protocol, both the server and user verify the identity of the other. This can be important when it is essential to be certain that the URL address is not diverting to another site, for example, when logging in to a bank application.

### Authentication Security and Efficiency

Both symmetric and asymmetric protocols provide equal security, assuming that neither database is compromised. Both protocols provide a high level of security that is as strong as the algorithm and keys used.

Symmetric key algorithms are far more efficient than asymmetric. However, since symmetric protocols involve computing only a single key signature, the differences in efficiency are less significant.

Secure authentication requires secure hardware, and it is in this context that we find the main advantage of symmetric over asymmetric protocols. Since symmetric key algorithms are much simpler than asymmetric, the hardware required is significantly less expensive.

### **Authenticated Key Exchange**

The use of tokens for authentication provides a high-security solution for preventing impersonation. However, for many applications, impersonation is only a small part of the problem. Aside from the fact that messages sent after the authentication stage may be read by an eavesdropper, they can also be modified.

In order to solve this problem, the authentication stage is followed by a key exchange protocol that provides both parties with a joint secret key. This key is used for encrypting and validating the integrity of all messages sent during a communication session.

The key exchange protocol is not separate from the authentication protocol, which is why this protocol is often called authenticated key exchange. This operation cannot be performed with challenge-response cards, but requires hardware capable of executing cryptographic operations.

The comparison between symmetric and asymmetric methods regarding key exchange protocols is almost identical to the comparison relating to authentication. Therefore it is safe to say that symmetric tokens are more advantageous, because they provide the same level of security at a much lower cost.

Disk encryption is an essential precautionary measure that is particularly valuable to users whose laptop, or home or office desktop PC, may be lost or stolen. Disk encryption secures the contents of the file system.

However, the private key used to decrypt the disk can be vulnerable to hacking if stored on the computer itself. To prevent a hacker from tracking down and decrypting all files on the PC or laptop disk, the private key must be stored in a separate location.

To ensure enhanced security protection for the laptop or PC file system, an external device must be used, for example, a USB token that does not require additional hardware. For full security, all encryption should take place on the token.

For this application, asymmetric technology is simply not needed, because it is applied in the same way as a symmetric key solution.

On-token encryption provides the highest level of security, but at the expense of speed. A proven methodology has been developed for token-based disk encryption, called Remotely Keyed Encryption (see reference [BFN] on page 15). Remotely Keyed Encryption provides the same level of security as on-token encryption, with the speed and efficiency of encryption performed on the PC.

### Symmetric Smart Cards and Tokens

This section outlines the considerations relating to the choice of methodology for smart card applications, and of the most suitable algorithm for use with symmetric smart cards and tokens.

Smart cards enable users to sign and execute electronic transactions securely. The algorithm and keys reside inside a protected hardware device, and as a result are both secure and tamper-proof.

Most of today's smart cards are based on PKI asymmetric technology. For certain smart card applications, the full power of asymmetric technology is not needed. Solutions based on symmetric keys are inexpensive and efficient and provide the same security for the required application.

There is no need to use a full PKI-based smart card to secure a laptop or to provide remote authentication for restricted websites. A symmetric USB token provides a comprehensive, high-security solution with the functionality of a smart card, at a far more reasonable price.

### Choosing the Right Symmetric Key Algorithm

The Data Encryption Standard (DES) algorithm has proved itself over many years. However, its short key size makes it vulnerable to an exhaustive key search. The size of the key is 56 bits, which means that such an attack requires  $2^{56}$  (approximately  $7 \times 10^{16}$ ) operations. This may appear to be extensive, but with today's technology, this can be done in a reasonable amount of time.

Biham and Shamir (see reference [BS] on page 15) demonstrated how to attack DES using only  $2^{47}$  operations, instead of  $2^{56}$  for an exhaustive key search (approximately 1/500<sup>th</sup> of the time), but this also requires storing  $2^{47}$  plaintext/ciphertext pairs. This huge memory requirement makes this attack essentially impractical, leaving a brute-force exhaustive key search as the only known threat after years of research.

It is clear that DES is no longer a secure option. The Advanced Encryption Standard (AES) initiative by the National Institute of Standards and Technology (USA) aims to select a symmetric algorithm that can be securely used for many years to come.

## Alternatives to the DES Algorithm

A temporary solution is to use an extension of DES that effectively enlarges the key size. Triple-DES is the most well known of these methods, but it suffers from a reduction in efficiency. The main motivation for using symmetric key algorithms is efficiency, combined with the ability to use them on low-cost hardware. Although Triple-DES outperforms any asymmetric scheme, it significantly slows down operations.

Another option is DESX, a slightly modified version of the DES algorithm (see reference [KR] on page 15). First suggested by Rivest, DESX provides the efficiency of DES, with the addition of two exclusive operations by a whitening key to prevent an extensive key search. See reference [KR] for a more precise description of the algorithm.

J. Kilian and P. Rogaway have mathematically proved that, when no attack is executed on the internal structure of DES, the number of operations needed to break DESX is  $2^{118}$ .

After 20 years of attempted cryptanalysis, the best internal attack on DES requires obtaining  $2^{47}$  plaintext/ciphertext pairs, which is clearly impractical.

We therefore conclude that DESX is an excellent alternative to DES, combining efficiency and security with a known time-proven algorithm. Users should note that DESX is the technology chosen by Microsoft for the encrypted file system of Windows 2000.

## Encryption and eToken Functionality

A symmetric encryption token incorporating the DESX algorithm provides a highly functional, efficient, low-cost and portable security solution.

Aladdin has recently introduced *eToken R2*, the world's first USB-based token to use DESX technology. For more information about the Aladdin *eToken R2*, visit the Aladdin Security Portal at [www.eAladdin.com](http://www.eAladdin.com).

The following table summarizes the application issues discussed in this document and their recommended encryption methods:

<b>Application Issue</b>	<b>Symmetric Encryption</b>	<b>Asymmetric Encryption</b>
<b>e-Commerce</b>		√
<b>Ease of key management</b>		√
<b>Signature non-repudiation</b>		√
<b>Functionality</b>		√
<b>High-level security</b>	√	√
<b>Fast, efficient algorithm processing</b>	√	
<b>Key size</b>	√	
<b>Challenge-response</b>	√	
<b>Single-user security</b>	√	
<b>Disk encryption</b>	√	
<b>Mutual authentication</b>	√	
<b>Affordability</b>	√	

√ = Recommended

## **Encryption Application Summary**

## **Summary of Conclusions**

The following are the major conclusions presented in this paper:

- Asymmetric encryption provides more functionality than symmetric encryption, at the expense of speed and hardware cost.
- Symmetric encryption provides a cost-effective and efficient method of securing data without compromising security, and should be considered as the correct and most appropriate security solution for many applications.
- In some instances, the best possible solution may be the complementary use of both symmetric and asymmetric encryption.
- The DESX algorithm, used in conjunction with a symmetric encryption token, provides a highly efficient, low-cost and portable security solution.

This document is based upon the following research:

Ref	Research Document
[BFN]	M. Blaze, J. Feigenbaum and M. Naor, <i>A formal treatment of Remotely Keyed Encryption</i> . A preliminary version appeared at Eurocrypt '98.
[BS]	E. Biham and A. Shamir, <i>Differential cryptanalysis of the full 16-round DES</i> , Advances in Cryptology, proceedings of CRYPTO '92, pp. 487-496, 1992. A full version of the paper can be found at: <a href="http://www.cs.technion.ac.il/~biham/">http://www.cs.technion.ac.il/~biham/</a>
[KR]	J. Kilian and P. Rogaway, <i>How to protect DES against exhaustive key search</i> , Advances in Cryptology, CRYPTO '96, Lecture Notes in Computer Science, Vol. 1109, N. Koblitz, ed., Springer-Verlag, 1996, pp. 252-267. A full version of the paper can be found at: <a href="http://www.cs.ucdavis.edu/~rogaway/papers/">http://www.cs.ucdavis.edu/~rogaway/papers/</a>  A less technical summary of the above article by Phillip Rogaway was published in: <i>RSA Laboratories' CryptoBytes</i> , Summer 1996. The article can also be found at: <a href="http://www.cs.ucdavis.edu/~rogaway/papers/">http://www.cs.ucdavis.edu/~rogaway/papers/</a>
[L]	Y. Lindell, PHD student in the Foundations of Computer Science Group at the Faculty of Mathematics and Computer Science, the Weizmann Institute of Science, Rehovot, Israel: <a href="http://www.wisdom.weizmann.ac.il/~lindell/">http://www.wisdom.weizmann.ac.il/~lindell/</a>
	Cryptography definitions and reference information from RSA Laboratories can be found at: <a href="http://www.rsasecurity.com/rsalabs/faq/index.html">http://www.rsasecurity.com/rsalabs/faq/index.html</a>

## References