

Security Issues in E-commerce

Ramesh Sankaranarayana
Department of Computer Science
The Australian National University

Office: CSIT Building (108), room N220.
E-mail: ramesh@cs.anu.edu.au

Contents:

- Symmetric key cipher, DES.
- Asymmetric key cipher, RSA.
- Hash function and digital signatures.
- Key management problems.
- Internet security.

Why Security

Life security: Life insurance.

House security: Security doors, property insurance.

Vehicle security: Locks, alarms systems.

Car travel security: Safety belt, air bags.

Information security: Cryptography.

Computer system security: Fire-walls, access control, etc.

Network security: Security protocols.

Information hiding: Steganography.

What Are The Threats to Computer Systems?

- Unauthorised access.
- Denial of services.
- Information misuse.
- Reveal confidential information.
- Repudiation (deny what has been done).
- Stealing money !!!

Categories of Attack

- Interruption: Attack on Availability.
- Interception: Attack on Confidentiality.
- Modification: Attack on Integrity.
- Fabrication: Attack on Authenticity.

Another classification

- Passive Attacks:

- Release of message contents
- Traffic analysis

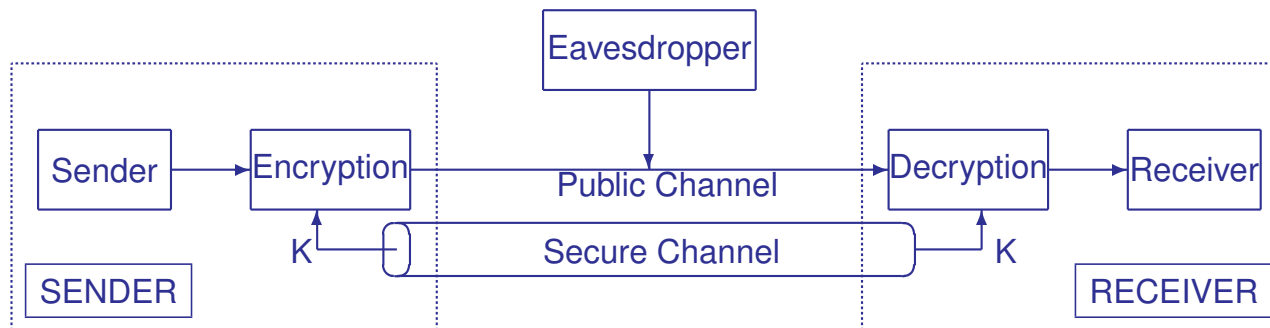
- Active Attacks:

- Masquerade
- Replay
- Modification of message contents
- Denial of service

What Can Security Techniques Do?

- Encryption: protect information confidentiality.
- Signature: provide authentication and non-repudiation services.
- Protocols: manage and control network security.

Basic Model of Secure Communications



Security Algorithms

- Symmetric key cryptography (with secret key).
 - Both sender and receiver have the same secret key.
 - Encryption on message m is done as $c = E_k(m)$.
 - Decryption on ciphertext c is done as $m = D_k(c)$.
 - Property: $D_k(E_k(m)) = m$ for any valid message m .
 - Note: $E_k(D_k(m)) = m$ is not always true.
- What are $E_k()$ and $D_k()$?
 - Mathematical transformations.

Security Algorithms

- ▶ Asymmetric key cryptography (with public key and private key).
 - ▶ Encryption and decryption use different keys, and may also use different algorithms.
 - ▶ May have digital signature functionality.
- ▶ Strength of cryptography (how hard it is to break a system)
 - ▶ Computationally secure vs unconditionally secure (statistically secure).
 - ▶ Depends on available algorithms, hardware and software performance.
 - ▶ Normal computational complexity is hundreds to millions of years of computation (for brute force attack).

Symmetric Key Cryptography

Stream cipher: $c = m \oplus k$, bit-by-bit or byte-by-byte x-or.

Example:

e	l	e	c	t	r	o	n	i	c	c	o	m	m	e	r	c	e
m	y	k	e	y	m	y	k	e	y	m	y	k	e	y	m	y	k
<hr/>																	
Q	J	O	G	R	D	M	X	M	A	O	M	W	Q	C	D	A	O

Block cipher: $c = f(m, k)$, encryption in blocks.

Example: cipher(15)(24)(36) = **EHRICP**.

Message too long? Chop off into shorter pieces.

QUESTION: How to decrypt a cipher? (cipher must be reversible).

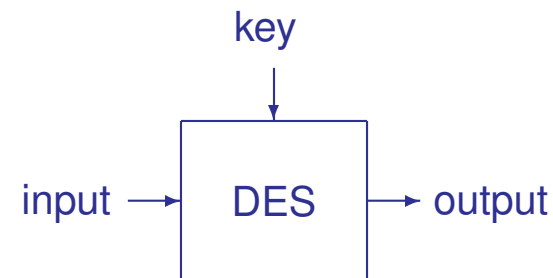
Data Encryption Standard (DES)

- A symmetric key cipher.
- Developed by US National Bureau of Standard (NBS) in 1970-75.
- 1976: it was adopted as a federal standard – DES.
- 1981: ANSI approved DES as private sector standard.
- 1983: DES was recertified, mainly for commercial use.
- revised every 5 years.
- 1998: not recommended, as it is not secure enough.
- 2000: Advanced Encryption Standard (AES) was adopted by US as replacement of DES.

DES Features

- Use 56-bit key (initial design was to use 128-bit key).
- Security relies only on the key, i.e. algorithm is public.
- Design complexity for breaking the system is 2^{56} trials, and the best known algorithm known so far (differential analysis) is not much faster (faster by a small factor).

- It encrypts 64-bit block of message into 64-bit block of ciphertext.



DES algorithm

- Input is re-ordered using an initial permutation (IP).
- Block is then split into two sub-blocks.
- It then follows 16 rounds of encryption.
- In each round of encryption, the left half is the old right half, and the

new right half is

$$R_{i+1} = L_i \oplus f(R_i, K_{i+1}).$$

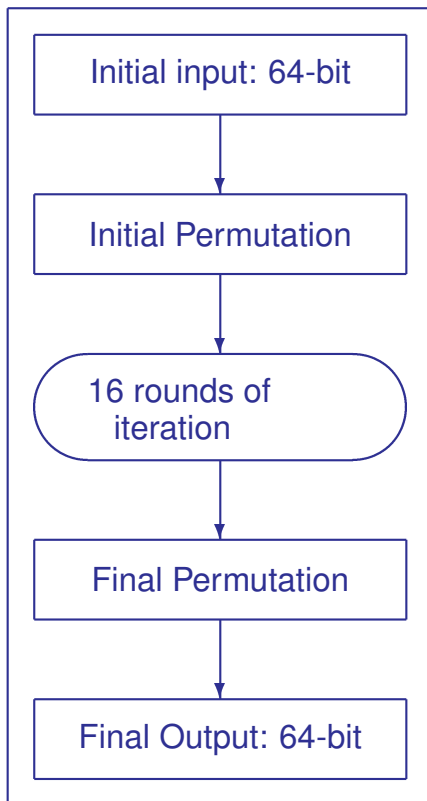
- In each round a 48-bit sub-key is generated and used.
- In general, the iteration algorithm looks like

$$L_i = R_{i-1}$$

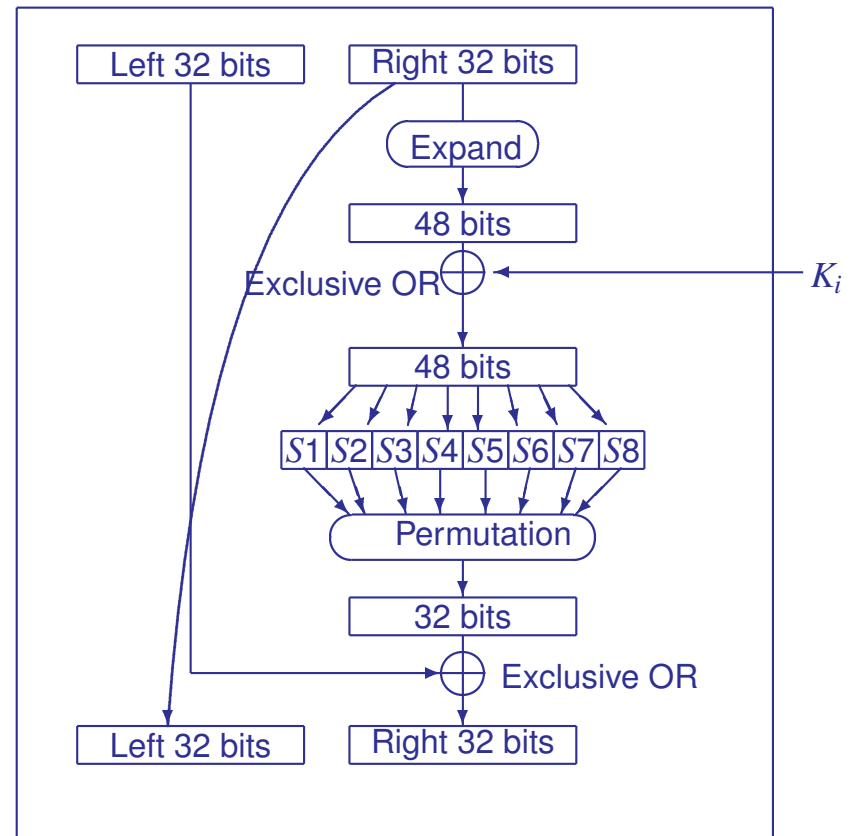
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

DES Algorithm

DES algorithm flowchart



Processing for Round i



How Hard to Break DES

- By trying all of the 2^{56} possible keys, one can certainly find the encryption key.
- For some of the properties of DES, the number of keys to be tested can be half of that, i.e. 2^{55} tries is enough. On average, the expected number of tries is $2^{54} = 18014398509481984$.
- Using the best known cryptanalysis algorithms, number of tries may be reduced, but cannot guarantee the key being found.
- In July 1998, the Electronic Frontier Foundation (EFF) announced the construction of a DES brute-force hardware cracker, DES Cracker. Cost less than US\$250,000. Average time to crack a DES key - 4.5 days.
- In January 1999, DES Challenge III cracked by DES Cracker and a network of around 100,000 PC's on the Internet, in 22 hours and 15 minutes.

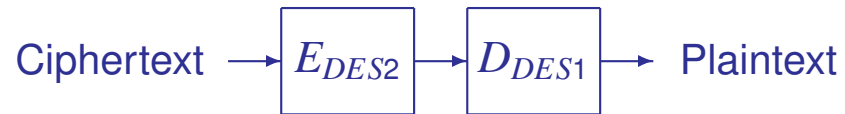
Double-DES and Triple-DES

- Double-DES: uses DES twice with different keys.

Encryption:

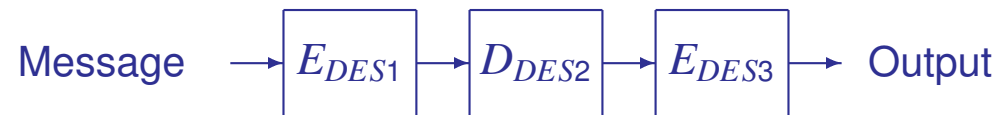


Decryption:



- Triple-DES: uses three concatenated DESs with different keys.

Encryption:



Decryption:



Advanced Encryption Standard (AES)

- October 2, 2000: The National Institute of Standards and Technology (NIST) announced that **Rijndael** has been selected as the proposed Advanced Encryption Algorithm (AES).
- The Secretary of Commerce approved the adoption of the AES as an official Government standard, effective May 26, 2002.
- Other candidates for the AES in the final round:
 - **MARS, RC6, Serpent, Twofish**
- Key size: can be 128, 192 or 256 bits.
- Block size: 128 bits.
- Number of rounds of iteration: 9, 11 and 13 respectively for different key lengths.

AES vs DES

- AES is faster than DES.
- AES is more secure than DES given that its larger key size.
- AES is more flexible for differing security requirements, since it has three key size choices.
- AES is by no means the best in any aspect compared with other block ciphers (particularly those candidates), but meets the requirement of US government.
- Criteria of selecting a good cipher:
 - security (based on primary analysis)
 - speed (hardware and software implementation)
 - ease of implementation (simple mechanism)
 - flexibility (e.g. use of different key lengths) etc.

Where to Find Further Information?

Reference books:

- S.Garfinkel and G.Spafford, **Web Security & Commerce**, O'Reilly, 1997.
- B.Schneier, **Applied Cryptography, Protocols, Algorithms, and Source Code in C**, John Wiley & Sons, 2nd Edition, 1996.
- C.P.Pfleeger, **Security in Computing**, Prentice Hall, 2nd Edition, 1997.
- W.Ford, M.S.Baum, **Secure Electronic Commerce**, Prentice Hall, 1997.

Reference URLs:

- <http://www.rsasecurity.com/>
- <http://csrc.nist.gov/encryption/aes/>
- <http://www.digicash.com/>
- <http://www.ecash.com/>
- <http://www.ecommerce.gov/>
- Use the search engine to find more.