Seminar On CRYPTOGRAPHY

Presented By Intramantra Global Solution PVT LTD, Indore
http://intramantra.com
WHAT IS CRYPTOGRAPHY?

- It is derived from two Greek words –
  “KRYPTOS” means secret and “GRAPH” means writing.

- It is art and science of keeping messages secure.
TERMS INVOLVED IN CRYPTOGRAPHY

- INTEGRITY.
- CONFIDENTIALITY.
- AUTHENTICATION.
- NON-REPUDIATION.
OVERVIEW

- Plain Text
- Cipher Text
- Cryptanalysis
- Cryptanalyst
- Cryptology
- Encryption
- Decryption
**ENCRYPTION:**
Procedure to convert plain-text into cipher-text.

**DECRIPTION:**
Procedure to convert cipher-text into plain-text.
TYPES OF ENCRYPTION

● SYMMETRIC ENCRYPTION

Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

plaintext $\rightarrow$ ciphertext $\rightarrow$ plaintext

● ASYMMETRIC ENCRYPTION

Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

plaintext $\rightarrow$ ciphertext

hash function
SYMMETRIC KEY CRYPTOGRAPHY

- Both ends of message channel have same key
- Key size measured in bits

Diagram:
- Plaintext
- Encryption
- Key
- Decryption
- Ciphertext
SYMMETRIC KEY CRYPTOGRAPHY

Dear General:
We have learned that...

Secret key method

Sender uses secret key

Recipient uses same secret key

Dear General:
We have learned that...

XdrrgbrnilkjlkUiu7d748#ookoiu...oi.9n5uoisafdlkj
DES

- Data Encryption Standard
- Has a 64-bit block size
- DES works on 64 bits of data at a time.
- Uses a 56-bit key during execution.
- Uses 16 Rounds.
APPLICATIONS

- Computer password.
- ATM security.
- Military security
- Electronic commerce.
- Authentication of messages.
- Digital signatures.
- Interactive proofs.
- Secure computations.
CONCLUSION

With the introduction of computer, the need for automated tools for protecting files & other information stored on the computer, to protect these type of files & our network we use cryptography.
BIBLIOGRAPHY

Books
Practical Cryptography - Bruce Schneider, Niles Ferguson.

Websites
www.google.com
www.howstuffworks.com