

Introduction to Cryptography

**Prepared for
COMMON Fall 1996**

Vincent LeVeque, Manager
Science Applications International Corporation (SAIC)
October 1996

CONTENTS

1	What is Cryptography?
2	Some Uses
3	History
4	Protocols
5	Public vs. Private Key Systems
6	DES - Data Encryption Standard
7	RSA - Public Key Encryption
8	PGP - Cryptography for the Masses
9	AS/400 Products

CONTENTS

10

More Information

WHAT IS CRYPTOGRAPHY?

- Crypto = secret; Graphy = writing
- The art of keeping messages secure
- "Exchanging a lot of small secrets for one big secret"
- Cryptography helps provide:
 - Authentication
 - Data Integrity
 - Privacy
 - Non-Repudiation
- Related areas of study:
 - Cryptanalysis - science of uncovering secrets
 - Cryptology - mathematics of cryptography and cryptanalysis

WHAT IS CRYPTOGRAPHY?

Cryptography Definitions

- Plaintext - The “in the clear” message, prior to encryption
- Ciphertext - Plaintext which has been encrypted
- Key - A secret or protected value used by the encryption algorithm to create ciphertext from plain text.
- Keyspace - The set of all possible keys for a given encryption algorithm.
- Key Management - The process of generating, distributing, storing, and destroying cryptographic keys.
- Algorithm - The method used to encrypt plaintext. The method is not assumed to be secret.
- Protocol - A specified series of steps, performed by two or more parties, in order to accomplish a task.
- Code - Cryptosystem that deals with linguistic units - words, phrases, etc.
- Permutation Cipher - A cipher which “shuffles” or recombines the elements of plaintext (characters or bits) to make ciphertext.
- Substitution Cipher - A cipher which substitutes plaintext (bits, bytes, or other patterns) with something else to make ciphertext.

CRYPTOGRAPHY USES

Military/Diplomacy:

- Strategic and tactical communication
- Secrecy

Banking

- Automated Teller
- Electronic Funds Transfer

Electronic Commerce:

- EDI message authentication and encryption

Data Processing:

- Password Validation
- Verifying Operating System Integrity

CRYPTOGRAPHIC HISTORY

- Diplomacy - 17th Century European Black Chambers
- Commercial Telegraphy
- Military (Signal) Telegraphy
- Radio Communications - W.W.I
- Cipher Machines - W.W.II German Enigma

CRYPTOGRAPHIC PROTOCOLS

- Secret Messages
- Subliminal Channel
- Key Distribution/Key Management
- Secure Hash
- Digital Signatures
 - Designated Confirmer Signatures
 - Undeniable (or non-transferable)
 - Proxy Signature
- Secret Sharing ("Threshold Scheme")
- Fair Coin Flips
- Key Escrow (a type of threshold scheme)
- Zero Knowledge Proofs

PUBLIC VS. PRIVATE KEY

- Private = Symmetric Key
 - Encryption key is same as decryption key
 - Traditional, used for centuries
 - Key management is problematic
 - Computationally fast

PUBLIC VS. PRIVATE KEY

■ Public = Asymmetric Key

- Public discovery in mid 1970's (NSA claims earlier discovery)
- Encryption key is separate from decryption key
- Encryption key is publicly distributed, decryption key is secret
- Simplifies key management
- Inverse process provides for digital signature
- Susceptible to "chosen plaintext" attacks
- Slow, very compute intensive

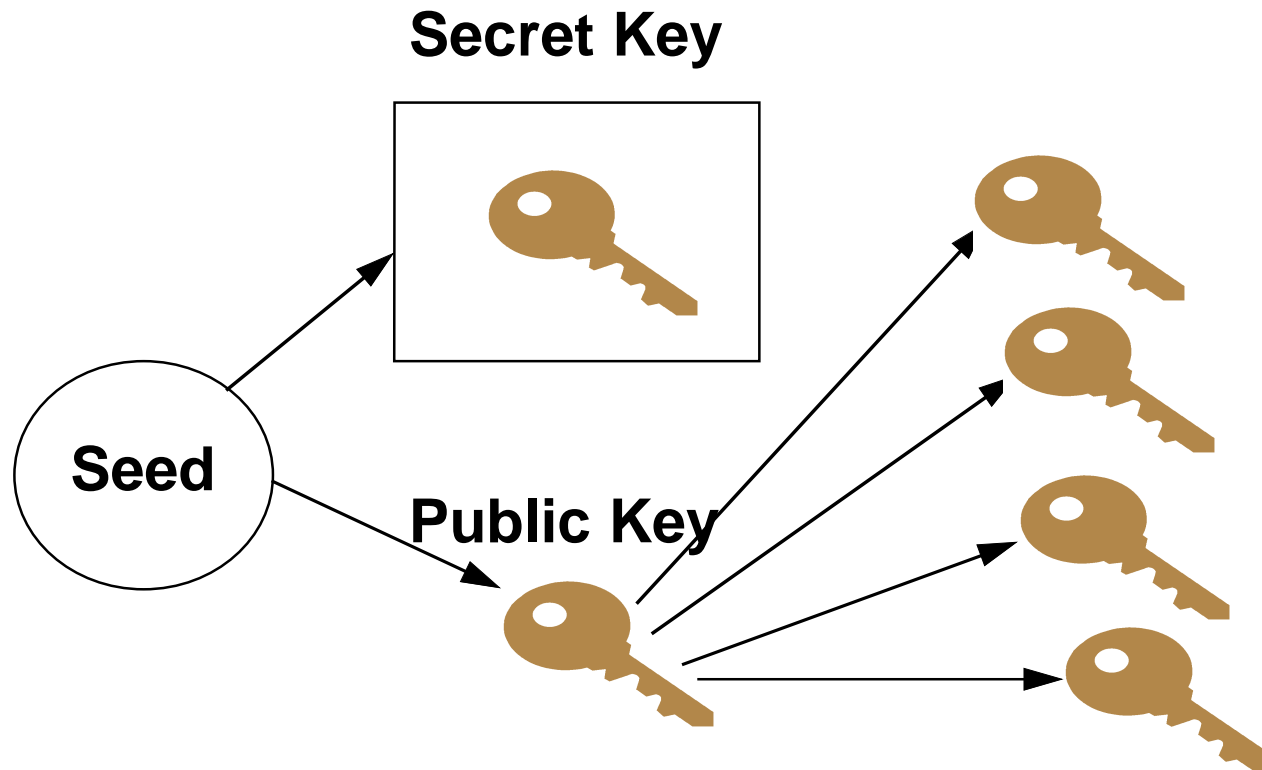
PUBLIC VS. PRIVATE KEY

■ Private Key protocols

- Key Generation - Results in creation of two mathematically related keys
- Key Distribution - The public or encryption key is distributed widely. Requires a Certification Authority to prevent key spoofing. Key distribution is otherwise public and unprotected.
- Encryption - Encryption is done with the public key. Anyone with the public key may encrypt.
- Decryption - Decryption is done using the private key retained by the owner. This key must be kept secret, or the whole system is compromised

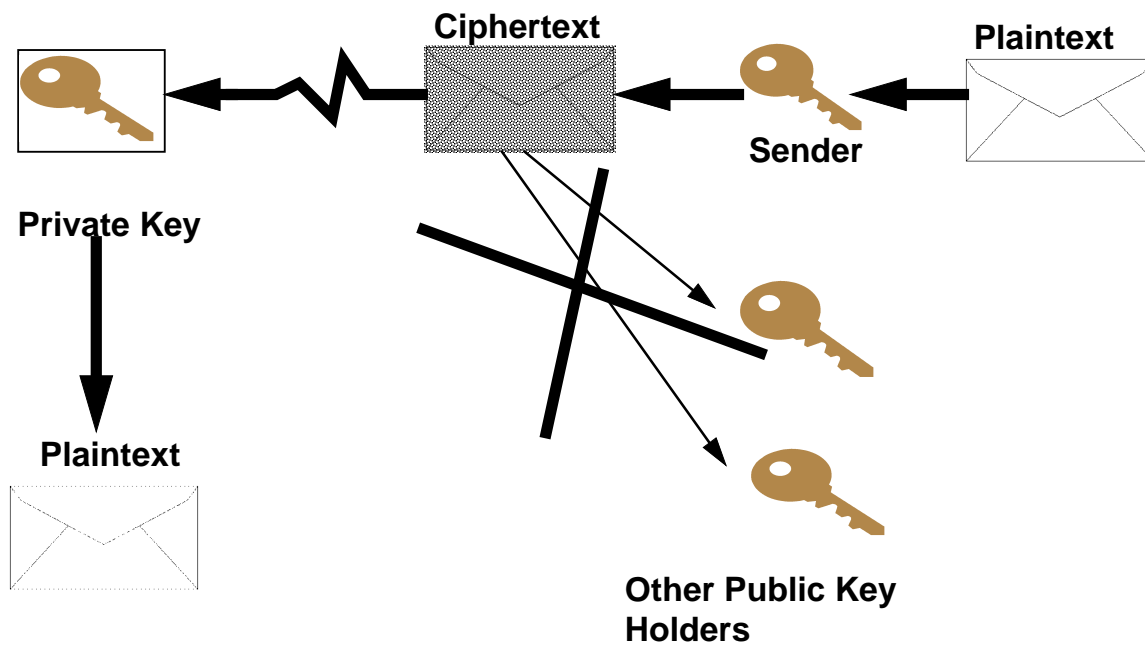
PUBLIC VS. PRIVATE KEY

- Public Key Protocols - Key Generation & Distribution



PUBLIC VS. PRIVATE KEY

■ Public Key Protocols - Encryption & Decryption



PUBLIC VS. PRIVATE KEY

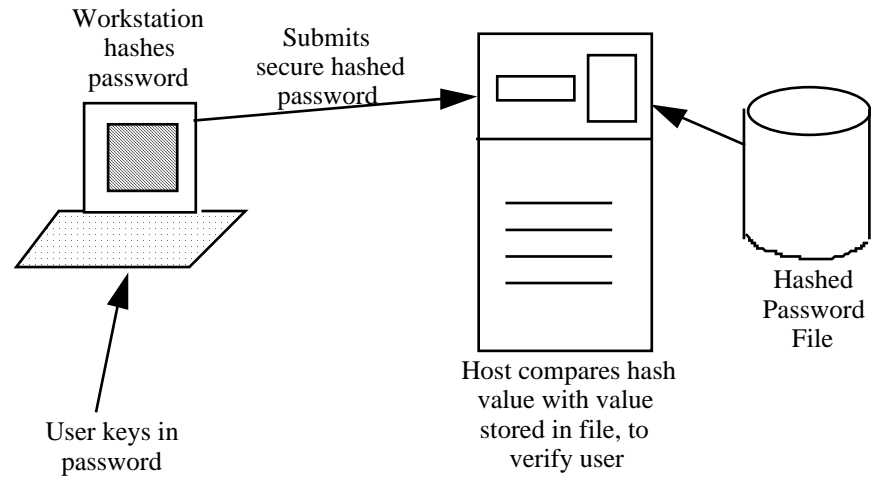
■ More Public Key Protocols - Digital Signatures

- Key Generation - Same as with encryption
- Key Distribution - This time the secret key, or the decryption key is distributed. The public or encryption key is kept secret.
- Message Signing - The sender encrypts with the public key.
- Signature Validation - The recipient decrypts using the public key. Successful decryption verifies that only the key owner could have created the message.

To save space and computation time, usually only a message digest or secure checksum is signed. The recipient validates the checksum against that of the plaintext message to verify signature.

PUBLIC VS. PRIVATE KEY

■ A Secure Hash Protocol - Password Validation



ENCRYPTION ALGORITHMS

Method used for generation of ciphertext from plaintext

- Data Encryption Standard (DES)
- RSA public key
- IDEA
- RC5
- Skipjack (used in Clipper chip)
- Digital Signature Algorithm (DSA)
- Secure Hash Algorithms
 - MD5
 - SHA

ENCRYPTION ALGORITHMS

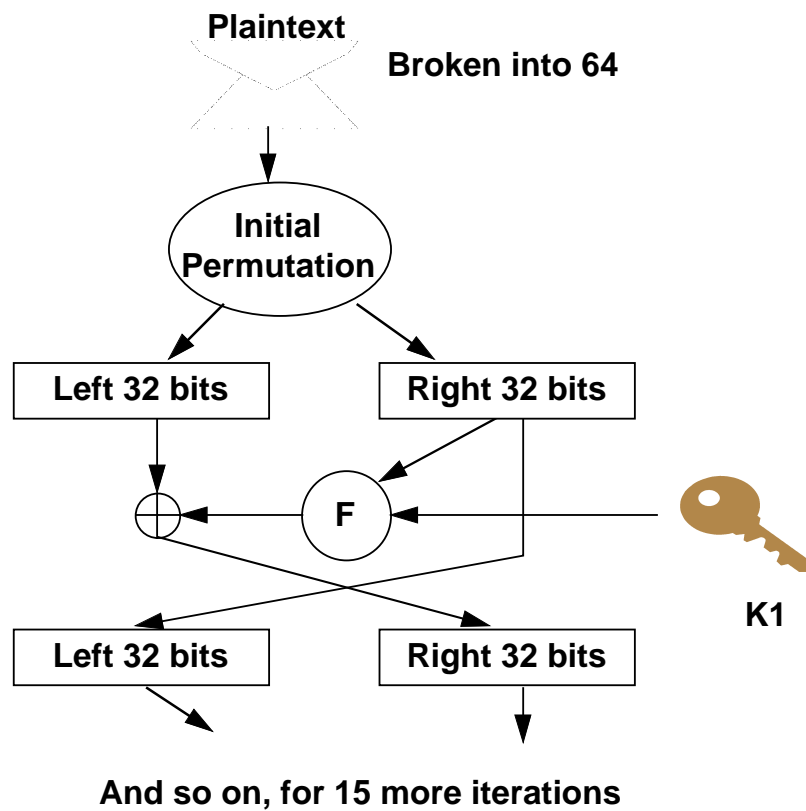
Breaking Encryption

- Passive vs. Active Attacks
- Protocol Subversion
 - “Man in the Middle”, third party takeover of key exchange
- Ciphertext Only
- Known Plaintext
- Chosen Plaintext
- Brute Force Key Generation
- Traffic Analysis
- “Rubber Hose” Cryptography
 - Bribery
 - Social Engineering
 - Other

DATA ENCRYPTION STANDARD - DES

- Began as IBM's Lucifer algorithm
- Approved as standards in FIPS Pub 46 and other FIPS documentation
- Most common commercial encryption algorithm.
- Designed for fast hardware implementation, given mid-1970's technology.
- Combines permutation and substitution in a bitwise fashion against 64-bit blocks of a message.

DATA ENCRYPTION STANDARD - DES



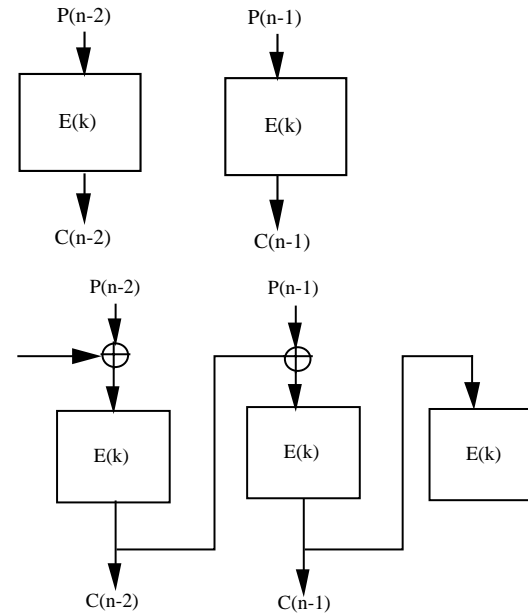
DATA ENCRYPTION STANDARD - DES

DES Modes

■ Block Modes:

○ Electronic Codebook (ECB)

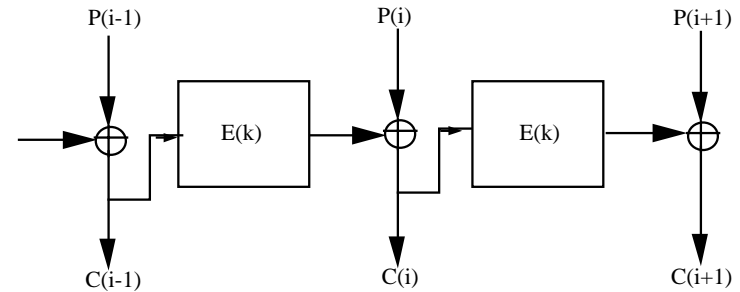
○ Cipher Block Chaining (CBC)



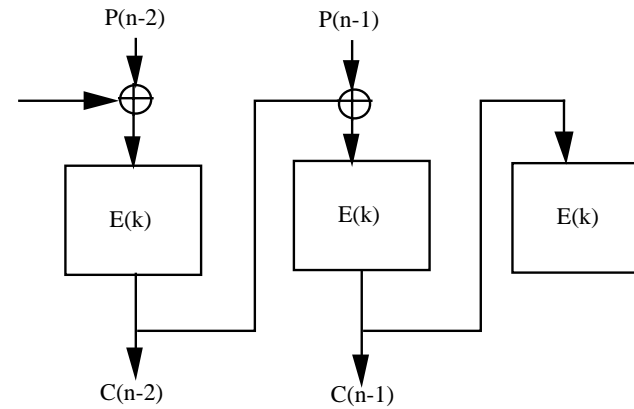
DATA ENCRYPTION STANDARD - DES

■ Stream Modes:

○ Cipher Feedback (CFB)



○ Output Feedback (OFB)



DATA ENCRYPTION STANDARD - DES

- Modes have different cryptographic characteristics:
 - Cryptanalysis vulnerabilities
 - Error propagation
 - Speed of encryption/decryption
 - Sequential vs. non-sequential data access

DATA ENCRYPTION STANDARD - DES

DES future

- Limitations of 56 bit key
- Periodic reviews, recertification every 5 years by the National Bureau of Standards
 - 1987 - Proposal to replace with Commercial Comsec Endorsement Program
 - 1993 - Still re-certified, though alternatives to be considered over next 5 years
 - 1998 - ?
- Lack of standard alternative
- Triple DES - interim solution

RSA - PUBLIC KEY ENCRYPTION

Elements of RSA

- RSA = Initials of inventors (Rivest, Shamir, Adelman)
- RSA has been widely licensed by a variety of companies.
- Patents never successfully challenged.
- Patents expire 1999.
- RSA acquired by Security Dynamics in 1996.
- Secrecy is based on the difficulty of finding prime factors of very large numbers.

RSA - PUBLIC KEY ENCRYPTION

Products Using RSA

- RSA has been widely licensed by a variety of companies.
 - ViaCrypt - Commercial version of PGP. Permits Key Escrow.
 - Verisign - A private Certification Authority.
 - Premenos - Templar product uses RSA to conduct secure EDI transactions over the Internet.
 - V-One - Token-based secure transaction over the Internet.
 - Pitney Bowes - Veritas Authentication System, to authenticate printed documents through bar-coded digital signatures.
 - Frontier Technologies - Secure WWW and TCP/IP tools
- RSA public key encryption is embedded in a variety of common software products.
- RSA's BSAFE encryption engine permits developing applications using a variety of strong encryption algorithms.
- PKCS is an industry-wide standard for developing public key applications

PGP - ENCRYPTION FOR THE MASSES

- Freeware, widely available on the Internet
- Combines Public Key (RSA) and Private Key (IDEA) algorithms
- Free version is non-commercial use only per licenses
- Legal issues
 - Patents
 - Export restrictions
- Recently ported to the IBM AS/400 by Steve Glanstein.
- See COMMON Lab session on the use of PGP for an excellent introduction.

AS/400 CRYPTOGRAPHY PRODUCTS

- Cryptographic Support/400
 - Software only
 - Licensed program product, available since AS/400's inception
 - Provides encryption of files and communications
 - Uses DES in Cipher Block Chaining mode
 - Provides key management and key secrecy through the host master key and the cross domain keys
 - Includes Personal Identification Number (PIN) functions (limited)
 - Provides CL command interface for cryptographic functions
- Common Cryptographic Architecture Services/400 (CCAS/400)
 - Software and hardware options included
 - Stores key in IOP tamper resistant module
 - Supports public key encryption
 - Used in environments which require storing key in hardware (banking)
- LU6.2 Session Level Encryption
 - Software only
 - Requires PRPQ and hardware device
 - Easy to use with existing LU6.2 applications

AS/400 CRYPTOGRAPHY PRODUCTS

- Secure Sockets Language
 - Provided in V4R1

AS/400 CRYPTOGRAPHY PRODUCTS

Other Host-based AS/400 Cryptographic Products

- Prime Factors
 - DESCRYPT +
 - DESCRYPT/EDI + - FDESMAC +
- Arkansas Systems - DES-Mate

AS/400 CRYPTOGRAPHY PRODUCTS

Communication Link Encryption

- Modems
 - Western Datacom - DES encryption modems, including 500 Series rack-mounted and 600 series standalone
 - CDI - DES-Guard portable encryptor and a variety of other products
- Routers
 - UUNET - LAN Guardian
- Spread Spectrum in Microwave Communications

AS/400 CRYPTOGRAPHY PRODUCTS

Mass Storage Encryption

- Contemporary Cybernetics - Backup media (tape) encryption

AS/400 CRYPTOGRAPHY PRODUCTS

User Authentication - Replacing the Reusable Password

- S/Key
- Kerberos - Part of OSF Distributed Computing Environment (DCE)
- Public Key Encryption
- Time-based Physical Tokens
 - Security Dynamics SecureID product
- Challenge/Response Physical Tokens
 - LeeMah Datacom Security - InfoKey
 - Racal-Guardata - Watchword
 - Information Research Engineering - AX200 Encrypting Token
 - Encotone - TeleID
- Biometrics
 - Veritel - Caller Verification System

SELECTING AND IMPLEMENTING CRYPTOGRAPHY

- Establish business needs and requirements.
- Select products using publicized algorithms, tested by expert cryptanalysts
- Pay careful attention to key generation and management.
- Ensure recovery of data if key lost.
- Ensure solid procedures and policies underlie cryptographic protocols.
- Ensure consistent security architecture throughout - don't put a steel door on a grass hut.

SECURITY PRODUCTS AND SERVICES

■ Starters

- Applied Cryptography, Bruce Schneier, John Wiley & Sons, New York, ISBN 0-471-11709-9
- The Codebreakers, David Kahn, Macmillan Company, New York, 1967

■ Free with this seminar

- Cryptography FAQ (diskette)
- PGP FAQ (diskette)

■ AS/400 Products

- AS/400 Cryptographic Support/400 (SC41-3342-00)

■ For "True Propellerheads"

- Cryptography Theory and Practice, Douglas R. Stinson, CRC Press, Boca Raton, ISBN 0-8493-8521-0
- Cryptography and Data Security, Dorothy Denning, Addison Wesley, Menlo Park, 1983, ISBN 0-201-10150-5

SECURITY PRODUCTS AND SERVICES