# Cryptography

*Ed Crowley*
*Fall '05*



## Topics

- Cryptographic Services
  - Confidentiality
  - Integrity
  - Authentication
  - Non-repudiation
- Concepts, Methodologies, and Practices
- Sym vs. Asym
  - Secret Key Crypto
  - Public Key Crypto
- Algorithms
- Methods of Attack
- Hash Functions
- Message Authentication
- Digital Signatures
- Key/Key Management issues
- Public Key Infrastructure
- Cryptographic applications to protocols

## Why Learn Cryptography?

**Mary Queen of Scots**

1542 -- 1587

3

## Mary Queen of Scots

- In Jan 1586 while in prison, Mary began to receive smuggled letters.
  - Delivered by Gilbert Gifford.
  - The letters were enciphered with a nomenclator.
    - Somewhat analogous to a monalphabetic cipher with symbols replacing certain words.
- Letters were smuggled in a hollow beer bung.
  - A form of steganography
- Within the letters, what has become known as, the Babington Plot was proposed.

4

## Babington Plot

- Plot proposed by Anthony Babington and a small group.
- In essence the plot proposed to free Mary Queen of Scots, and assassinate Queen Elizabeth.
- At that point, it may have been possible for Mary to succeed her cousin as Queen of England.

5

## Gilbert was a Double Agent

- Queen Elizabeth's secretary intercepted the letters.
- Applied cryptanalysis.
  - Broke the code and became aware of the plot.
- To entrap the conspirators, the secretary also forged a postscript. In part, it read:

  *I would be glad to know the names and qualities of the six gentlemen which are to accomplish the designment; for it may be that I shall be able …, to give you some further advice …*

6

## Four Points

- When Gilbert turned out to be a double agent, the steganography no longer kept the messages hidden.
- When cryptanalysis was applied to the letters, their contents lost their confidentiality.
- When the opposition was able to add a post script, the letters lost their integrity.
- When the trial was over, Mary lost her head!
  - If she would have understood the limits of Cryptography, she might have kept her head!

7

## Cryptography Defined

> The principles, means and methods for rendering information unintelligible, and for restoring encrypted information to intelligible form.
>
> -- *Orange Book*

http://www.fas.org/irp/nsa/rainbow.htm

*Note*

- Security is a lot more than encryption.
- Privacy is a lot more than security.

8

## Goal

- Make obtaining or altering information too expensive, in time or money, to be worth it to an opponent.
- Encryption strength is context sensitive.
  - Related to the information's perceived value to the opponent.
- Cryptography doesn't have to be perfect, it just has to be stronger than your opponent's attack methods and resources.

9

## Four Cryptographic Services

- Confidentiality -- Encryption
  - Only authorized people –e.g., the sender and recipient of a message, not eavesdroppers – can know the message.
- Integrity – Digital Signatures
  - When Bob receives a message, he can be sure that it was not modified en route after Alice sent it.
- Authentication – Digital Signatures
  - When Bob receives a message that purports to be sent by Alice, Bob can be sure that the message was really sent by Alice.

10

## Four Cryptographic Services

- Nonrepudiation -- Digital Signatures
  - Alice cannot later deny that the message was sent. Bob cannot later deny that the message was received.

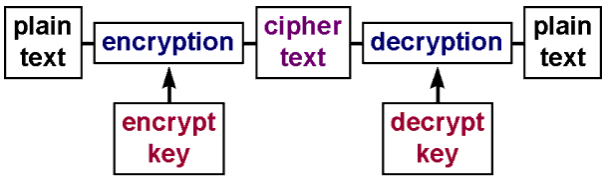
11

## Secret Writing Roots

- Cryptography, like steganography, is a branch of secret writing.
- Like steganography, it grew out of a need for confidentiality.
- Codes, in contrast to ciphers, are also a branch of secret writing.
  - Differ from ciphers in that codes work at the word level, while ciphers work at the character level.

12

# Encryption Process




**Encrypt Key = Decrypt Key**
**Symmetric Keys**

**Encrypt Key != Decrypt Key**
**Asymmetric Keys**

13

# Selected History

- In the fifth century BC, Cicero reported that secret writing saved the Greek states from the Persians.
  - 400 BC, Spartans employed military cryptography in the form of a strip of papyrus or parchment wrapped around a wooden rod. *(Scytale cipher)*
- 49 BC, Julius Caesar used substitution ciphers.
- In 9th century Baghdad, the First recorded cryptanalysis of a monoalphabetic cipher was recorded.

14

## Selected History

- Monoalphabetic ciphers continued to be widely used until the 16th century.
  - 16th century, polyalphabetic (Vigenere) cipher was invented.
- 1790, Thomas Jefferson developed an encryption device using a stack of 26 disks that could be rotated individually.
  - Equivalent to a Vigenere cipher with a key length of 36.

15

## Selected History

- 1883, Kerckhoff's Principle
  - The security of a cryptosystem must not depend on keeping secret the crypto algorithm. The security depends only on keeping the key secret.
- 1920, Herbert Yardley and the American Black Chamber.
  - Some consider Yardley to be the Father of American Cryptography.

16

## Selected History

- 1917, One Time Pad
  - Only cryptographic methodology that can be proven to be unbreakable (when implemented correctly).
    - Key management issues make it almost impossible to implement correctly.
  - A special type of Vigenere cipher where the key is the same length as the message.
    - To be effective, the key must only be used once.
    - The key's components must be truly random and have no periodicity or predictability.

17

## Selected History

- 1920, William Frederick Friedman published The Index of Coincidence and Its Applications in Cryptography.
  - Index of coincidence is a statistical measure of text which distinguishes text encrypted with a simple substitution cipher (aka a monoalphabetic cipher) and more complicated Vigenere methods (aka polyalphabetic ciphers.)
  - Some consider Friedman to be the "Father of Modern Cryptography".

18

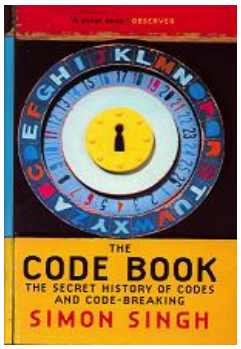
## Selected History

- 1933—1945, German Enigma
  - A polyalphabetic substitution cipher machine.
  - Cracked by British at Benchly Park
- Unix uses a substitution cipher called ROT 13 that shifts the alphabet by 13 places.
  - `http://www.rot13.com/index.php`
- 1970, IBM and Feistel develop Lucifer.
  - Later, evolved into DES.
- 1976, Diffie –Hellman--Merkle Public Key Encryption
- 1991, PGP Phil Zimmerman
- 2000, AES wins NIST competition.

19

## Selected History

For a good historical presentation see: Simon Singh's: "The Code Book" :




http://www.simonsingh.net/Crypto_Corner.html

20

## Selected Terms

- Stenography
  - Secret communications where the existence of the message is hidden.
- Work Function (factor)
  - Measure of difficulty in recovering plaintext from cipher text.
    - Measured by cost and/or time.
  - Another name for work factor is encryption method strength.

21

## Cryptographic Terms

- Algorithm
  - A well-defined procedure or sequence of steps used to produce a key stream or cipher text from plain text and vice versa. *(Orange Book)*
- Block Cipher
  - Obtained by segmenting plaintext into fixed size blocks and applying the identical encryption algorithm and key to each block. *(Contrast with stream cipher.)*
- Block Chaining
  - Parts of previous block are inserted into current block

22

## Cryptographic Terms

- Clustering
  - Situation when a plain text message generates identical cipher text messages using the same transformation algorithm but with different keys.
- Codes
  - A cryptographic transformation that operates at the level of words or phrases.

23

## Cryptographic Terms

- Cryptanalysis
  - The science of analyzing and breaking secure communication..
- Ciphertext
  - Plaintext that has been encrypted.
- Decryption
  - Changing ciphertext back to plaintext.
- Key
  - Sequence of bits and instructions that governs encryption and/or decryption.

24

## Cryptographic Terms

- Keyspace
  - Range of values that can be used to construct a key.
- Key clustering
  - When a plaintext message generates identical ciphertext messages using the same transformation algorithm, but with different keys.
- Link Encryption
  - In the transmission chain, where each entity has keys in common with its two neighboring modes.
- Plaintext
  - Data that can be read and understood without any special measures aka cleartext.
- Stream cipher
  - Message broken into characters or bits and enciphered with a key stream. (Contrast with block cipher.)

25

## Vernam Cipher and One Time Pads

One time pad

- A special implementation of the Vernam Cipher with a key length same as message length.
  - Key must be random set of non repeating characters.
  - Each key must only be used one time for only one message. Must never be used again.
- If done properly, unbreakable.
- Considered impractical (Key management problems.)

http://www.pro-technix.com/information/crypto/crypto_frame.html

26

## Modern Ciphers

- Both substitution and transposition ciphers are vulnerable to frequency analysis attacks.
  - For several hundred years, polyalphabetic ciphers were considered unbreakable until Babbage and Kasiki proved otherwise.
- Consequently, most modern ciphers use long sequences of complicated substitutions and permutations.

27

## Cryptographic Technologies

Symmetric or Asymmetric key

- Symmetric key
  - aka secret or private key or single key cryptography.
- Asymmetric key
  - aka public key or two key cryptography.

28

## Symmetric Key

- Classic cryptography
- Utilizes identical Decryption and encryption keys.
- Fast
  - Up to 1,000 times faster than public key cryptography.
  - Ideal for bulk encryption
- (Key) Problems
  - Can only be used by prearrangement.
  - Problematic key management.
  - Does not scale well

29

## Asymmetric Key

- The new cryptography
- Utilizes two different, but related, keys.
  - Normally one Public key
  - And one Private key
- A message encrypted with one key can be decrypted with the other.
  - Slow
  - Solves key management problem associated with Classic Cryptography

30

## Symmetric Key Cryptography

- Provides confidentiality.
- Does not provide authentication or nonrepudiation.
- Single key, shared by sender and receiver.
  - aka conventional cryptography or single key cryptography.
  - aka Private Key Cryptography

31

## Symmetric Key Limitations

- Only works by prearrangement.
  - Whomever receives the information must already have the key.
- Key distribution and management is problematic.
  - How do you get the key to the recipient without someone intercepting it?
  - If two people have the key and it is compromised, whom is responsible?
  - If key is lost, cipher text cannot be decrypted.
- Does not scale well.

32

## Symmetric Key Cryptography

- Fast, up to 1000 times faster than asymmetric
  - Useful for encrypting large volumes of static data i.e. hard drives
- With large key sizes, can be very difficult to break.

33

## Symmetric Key Algorithms: DES

- Provided the first modern, secure symmetric encryption algorithm that was known in great detail, was free from patent rights, and enjoyed general acceptance.
- Relatively simple, uses only three functions
  - XOR
  - Permutation
  - Substitution

34

## Data Encryption Standard (DES)

- Symmetric key cryptosystem
  - 1972, derived from IBM's Lucifer algorithm
  - Originally designed for hardware implementation.
- Used for commercial and non-classified purposes.
- DES describes the Data Encryption Algorithm (DEA).

35

## DES Attributes

- A 16-round cryptosystem
- 56 bit key (Shorter than Lucifer!!!)
- 64 bit blocks.
- Since November 1998, not used by US government.
- Triple DES, replaced DES, and will be used until AES is adopted.

36

## Data Encryption Standard (DES)

- Implements confusion and diffusion for improving plain text encryption.
- Confusion conceals the statistical connection between cipher text and plaintext.
- Diffusion spreads the influence of a plaintext character over many cipher text characters.

37

## DES Modes

Four DES modes:

1. Cipher Block Chaining
2. Electronic Code Book
3. Cipher Feedback Mode
4. Output Feedback.

Cipher Block Chaining

- Operates with plaintext 64 bits blocks. For each block of text, the key and the value is based on the previous block . Consequently, identical patterns in different messages are encrypted differently.

38

## Electronic Code Book (ECB)

- Native DES mode
- Each 64 bit data block is encrypted independently.
- Each cipher text block corresponds to a plaintext block.
- When the same pattern occurs, it is always encrypted the same.
- Best suited for use with small amounts of data such as in a Data Base.

39

## Cipher Feedback Mode (CFB)

- Stream cipher where the ciphertext is used as feedback into the key generation source to develop the next key stream.
- Uses block chaining.
- Output Feedback
  - DES generated stream cipher that is XORed with a message stream.
  - Simulates a one time pad.

40

## DES Security

- Consensus is that DES is vulnerable to attack by a brute force search for the 56-bit key.
  - 1997, a distributed brute force attack (14,000 machines for 4 months, succeeded)
  - 1998, EFF demonstrated DES key cracking in 56 hours with a single $250,000 machine.
- Consequently, Triple-DES is currently in use.
- DES is scheduled to be replaced by AES (Advanced Encryption Standard)

41

## Triple DES

- Runs DES three times.
  - Uses two or three keys.
- Uses (16x3) 48 computation rounds
  - Highly resistant to differential cryptanalysis and approximately $2^{56}$ stronger than DES.
- Three times slower than DES.

42

## Advanced Encryption Standard

- Block cipher DES replacement.
- National Institute of Standards and Technology (NIST) initiative.
  - Announced January 1997.
- AES, aka the Rijndael Block Cipher
  - New Federal Information Processing Standard (FIPS) replacing DES.
  - US Government standard for protection of sensitive but unclassified information.

43

## Rijndael Block Cipher

- Iterated block cipher with variable block and key lengths that can be independently chosen as 128, 192, or 256 bits.
- Instead of a Feistel network that takes a portion of the modified plaintext and transposes it to another position, the Rijndael Cipher employs a round transformation that is compromised of three layers of distinct and invertible transformations.
- Design compared to other algorithms, relatively simplistic. (In security, simple is good.)

44

## Other Symmetric Ciphers (AES submittal)

- Two Fish
  - Developed by a team led by Bruce Schneier for entry into NIST's post DES competition.
- IDEA
  - International Data Encryption Algorithm used in PGP (patented)
- RC5
  - Fast symmetric block cipher with a variable word size, a variable number of rounds, and a variable-length secret key.

45

## Symmetric Key Management

- Problems with Symmetric Key Management led to the development of Asymmetric Key Cryptography.
- Note that most modern cryptosystems are hybrid systems that use both Symmetric and Asymmetric methods.

46

## Asymmetric Cryptography

- Employs a related pair of keys
  - One public, one private
  - aka Public Key Cryptography
- Based upon problems that are easy one way and very difficult the other
  - Factoring the product of two large primes (RSA)
    - Easy to multiply, very difficult to factor
  - Discrete logarithm problem
- Avoids key management problems associated with Symmetrical Cryptography.

47

## Asymmetric Cryptography Services

- Anyone with access to your public key can encrypt information that only you can read.
  - Confidentiality
- Only you can encrypt information with your private key.
  - Authentication
  - Non-repudiation

48

## Asymmetric Cryptography

- Public-key cryptosystems include:
  - Diffie-Hellman
  - RSA
    - Public key algorithm used for both encryption and digital signatures
  - Discrete Logarithm Signature Systems (DLSSs)
    - El Gamal
    - DSA, the Digital Signature Algorithm

49

## Key Size Comparisons

- An 80-bit private key has the equivalent strength of a 1024-bit public key.
- A 128-bit private key has the equivalent strength of a 3000-bit public key.

50

## Asymmetric Key Encryption Services

Confidentiality

Sender encodes message with receiver's public key. Receiver decodes with private key.

Authentication and Non repudiation

Sender encodes message with sender's private key. Receiver decodes with sender's public key.

51

## Cryptosystems

- Relative to classic cryptography, Public key cryptography is slow.
  - 1,000 to 10,000 times slower than secret key cryptography.
- Hybrid systems can use public keys to distribute secret (session) keys.
  - Symmetric key for bulk data encryption
  - Asymmetric key for key distribution
- Because of the computational intensity, working cryptosystems utilize symmetric key encryption for messages and asymmetric cryptography to pass the symmetric key

52

## One Way Functions

- Public key cryptography is possible through the application of a one way function.
- By definition, a one way function is easy to compute in one direction but difficult, or impossible, to computer in the reverse.
  - Factoring the product of two large prime numbers
  - Discrete logarithms
  - Elliptic Curve

53

## RSA

- Public key algorithm based on large prime numbers.
  - Based on the difficulty of factoring a number N, which is the product of two large prime numbers.
- Defacto world wide standard used for digital signatures and encryption.
- At the time of its publication, Rivest, Shamir, and Addleman were all MIT Professors.

54

## Diffie-Hellman Key Exchange

- Method where subjects exchange secret keys over a nonsecure medium without exposing the keys.
- Introduced the notion of public key cryptography.
- Used for key distribution cannot be used to encrypt and decrypt messages.
  - OAKLEY is a key establishment protocol based on the Diffie-Hellman algorithm and designed to be a compatible component of ISAKMP
    - Proposed for IPsec but superseded by IKE.
- Predates RSA.



## El Gamal

- Extended the Diffie-Hellman concept to apply to encryption and digital signatures.
- A non-patented public key cryptosystem based on the discrete logarithm problem.

## Elliptic Curve (EC)

- Elliptic curves are usually defined over finite fields such as real and rational numbers and implement an analog to the discreet logarithm problem.
- Smaller elliptic curve key sizes can yield higher levels of security.
- Requires less computational and memory requirements.

57

## Two Types of Public Key Algorithms

- Factoring the product of large prime numbers
  - RSA
- Finding the discreet logarithm in a finite field.
  - Elliptic Curve
- Examples of Public Key Crypto Algorithms :
  - El Gamal
  - Diffie-Hellman

58

## Cryptanalysis

- Science of cracking ciphers and codes, decoding secrets, violating authentication schemes, and in general, breaking cryptographic protocols.

59

## Cryptographic Attacks

- Objective is to be able to decrypt new pieces of cipher text without additional information.
  - An intermediate goal would be to crack the message key.
- Generally classified into categories that distinguish the kind of information the cryptanalyst has available with which to mount an attack.

60

## Attack Types

- Known Plaintext
- Chosen Plaintext
- Adaptive Chosen Plaintext
- Ciphertext Only
- Adaptive chosen plaintext
- Brute Force
- Birthday attack
- Meet in the Middle
- Man in the Middle
- Differential Cryptanalysis
- Statistical

61

## Cryptographic Attacks

- Ciphertext Only
  - Cryptanalyst obtains a sample of ciphertext, without the plaintext associated with it.
  - Most difficult type of attack.
    - Requires a very large ciphertext sample.
- Known Plaintext
  - Based upon a sample of ciphertext and the corresponding plaintext.
  - Could be part of message (repeating headers)

62

## Cryptographic Attacks

- Chosen Plaintext
  - Cryptanalyst can choose what plain text message he wishes to encrypt and view the results.
    - Much, much, stronger than known plain text attack.
  - Optimum type of attack.

63

## Cryptographic Attacks

- Adaptive Chosen Plaintext
  - Special case of chosen-plaintext attack in which the cryptanalyst is able to choose plaintext samples dynamically, and alter his or her choices based on the results of previous encryptions.

- A good algorithm must withstand a chosen plaintext attack, otherwise it is not secure.
- If known plain text or a cipher text only attack succeeds, then the algorithm should be discarded.

64

## Cryptographic Attacks

- Chosen-ciphertext
  - One in which cryptanalyst may choose a piece of cipher text and attempt to obtain the corresponding plaintext.
    - Generally utilized with public-key cryptosystems
- Adaptive-chosen-ciphertext
  - Scenario in which a cryptanalyst has free use of a piece of decryption hardware, but is unable to extract the decryption key from it.

65

## Brute Force Attacks

- Try every possible key until the correct key is identified.
- Advances in technology and computing performance will always make brute force an increasingly practical attack against fixed length keys.
- In certain contexts, a dictionary attack can be considered a form of brute force.

66

## Cryptographic Attacks

- Birthday attack
  - Usually applied to the probability of two different messages using the same hash function that produces a common message digest or given a message and its corresponding message digest finding another message that when passed through the same hash function generates the same specific message digest.



## Cryptographic Attacks

- Meet in the Middle
  - Applied to double encryption schemes by encrypting known plaintext from one end with each possible key and comparing the results in the middle.
    - Works brute force from both ends.
- Man in the Middle
  - An attacker taking advantage of the store and forward nature of a network by intercepting messages and forwarding modified versions of the original messages while in-between two parties attempting secure communications.

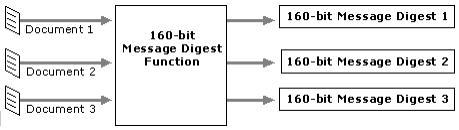
# Differential Cryptanalysis

- Differential Cryptanalysis
  - Attack that can be mounted on iterative block ciphers
  - Basically a chosen plaintext attack. Relies on an analysis of the evolution of the differences between two related plaintexts as they are encrypted under the same key.
  - By careful analysis of the available data, probabilities can be assigned to each of the possible keys, and eventually the most probable key is identified as the correct one.
- Statistical
  - Exploiting the lack of randomness in key generation.

69

# One Way Functions

- A hash is a one way function that can be used to provide message integrity services.
- Public Key Cryptography and hash functions provides the building blocks for Digital Signatures.




70

## SHA-1

- Any modifications to the message being sent to the receiver results in a different message digest being calculated by the receiver.
- When any message less than $2^{64}$ bits is used as an input, SHA-1 produces a 160 bit message digest.

71

## MD5

- Message digest algorithm, used in PGP.
  - Developed by Rivest in 1991.
- Generates a 128 bit message digest from an arbitrary length message.
- IETF standard (RFC 1321)

72

## HMAC

- HMAC, in conjunction with SHA-1 algorithm [FIPS-180-1], provides an authentication mechanism within the revised IPSEC Encapsulating Security Payload [ESP] and the revised IPSEC Authentication Header [AH].
- Provides data origin authentication and integrity protection.
- RFC-2104

73

## Message Digest Attributes

- Original file cannot be created from message digest (one way function).
- Given a file and its corresponding message digest, it should not be feasible to find another file with the same message digest.
  - This would be called a collision
- Should be calculated using all of the original file's data.

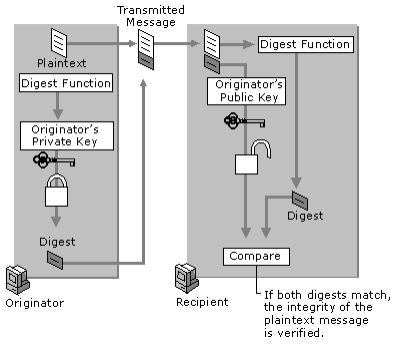
74

## Message Digests and Digital Signatures

- After a message digest is calculated, it is encrypted with the sender's private key.
  - This is the digital signature.
- The receiver can decrypt the message digest with the sender's public key.
  - If the public key opens the message digest, the senders identity is verified. (nonrepudiation)
- The receiver can re-compute the message digest.
  - If it hasn't changed the message has integrity.

75

## Digital Signatures




- Involves creation of a fixed length block of data (a Message Digest).
- The senders private key binds the fixed length block to:
  - The original data
  - The sender's identity.

76

## Digital Signature Standard (DSS) and Secure Hash Standard (SHS)

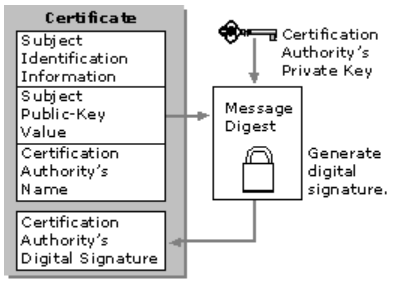
- Both digital signature algorithms use the Secure Hash Algorithm (SHA-1).
  - Defined in NIST's Federal Information Processing Standard (FIPS) 180.
  - Secure Hash Algorithm (SHA-1) computes a fixed length (160-bit) message digest from a variable length input message.
- A message digest is then processed by the DSA to either generate or verify a signature.

77

## Public Key Certificate Systems

Three parts of a digital certificate:

1. A public key.
2. Certificate information.
   - "Identity" information about the user, such as name, user ID…
3. One or more digital signatures.




78

## Public Key Certification Systems

- Include a certification process that binds individuals to their public keys.
- X.509 standard defines the format for public key certificates.
- The digital signature's purpose on a certificate is to state that the certificate information has been attested to by some other person or entity.
  - Trusted 3rd party concept

79

## Public Key Infrastructure (PKI)

- Integrates digital signatures, certificates, and the other services.
- Includes
  - Digital Certificates, Certificate Authorities
  - Registration Authorities, Policies and Procedures
  - Certificate revocation, Non-repudiation support

80

## PKI

- Also includes:
- Timestamping
- Lightweight Directory Access Protocol (LDAP)
  - Primary security concerns are availability and integrity of LDAP servers
- Security enabled applications
- Cross certification.

81

## Escrowed Encryption

- Idea is to divide the key into two, or more, parts and to escrow separate portions of the key with separate “trusted” organizations.
- When dealing with encryption keys, the same precautions must be used as with physical keys.

82

## Clipper Chip

- Government program to embed Clipper chips into electronic devices
- Based on an 80-bit implementation of the classified Skipjack algorithm
- Government would hold copies of keys in escrow for easy access by law enforcement
- Eventually died due to a lack of public support

83

## SET

- Developed by a consortium including MasterCard and Visa.
- Provides confidentiality for purchases by encrypting the payment information.
- Covers end to end transactions.

84

## SSL/TLS

- SSL was developed by Netscape to secure Internet client-server transactions.
  - TLS, an open standard, is SSLs successor.
  - Both provide confidentiality, authentication, and integrity above the transport layer.
  - Both use X.509 certificates.
- Does not provide protection for MIM attacks

85

## IPSec

- Standard that provides encryption , access control, non-repudiation and authentication of messages over IP.

Two main protocols are:

1. Authentication Header
2. Encapsulation Security Payload.

- AH provides integrity, authentication, and nonrepudiation.
- ESP provides encryption.

86

## IPSec

- A VPN implementation can operate in either transport or tunnel mode.
- Uses MD5 or SHA-1 hashing algorithms for authentication and integrity.
- Uses ISAKMP standard format (Internet Security Association and Key Management Protocol).

87

## Questions?

References One:

http://cis.gsu.edu/~rbaskerv/cis8680/Lessons/crypto/index.html

http://www.simonsingh.net/Crypto_Corner.html

http://www.schneier.com/

http://www-106.ibm.com/developerworks/library/s-pads.html

http://www.math.temple.edu/~renault/cryptology/affine.html

88

# References Two

https://www.isc2.org/cgi-bin/request_studyguide_form.cgi?AG=6042

http://www.microsoft.com/resources/documentation/windows/2000/server/reskit/en-us/distsys/part2/dsgch14.mspx

http://www.fas.org/irp/nsa/rainbow.htm

89

# Who am I?

- Developed four, three credit hour, UH Security Courses
- Past Security Presentations at: University of Indiana in Pennsylvania's Network Security Workshop, Infragard, ISACA, ACM SIGITE, and American Association for Engineering Education
- Earned CISSP, NSA IAM & IEM, Security Certifications
  - Usual certifications from usual suspects (Cisco, CompTIA, and Microsoft).
- Former IS Director
- Former Network Admin
- Graduate Military Police Academy
  - USARPAC German Shepard Sentry Dog School
  - Secret Clearance (expired)

90