_____ uses at least two different shifts, changing the shift with different letters in the plain text.

A Atbash

B multi-alphabet encryption

C Scytale

D Caesar cipher

B

____ was designed to provide built in cryptography for the clipper chip.

A Blowfish

B Skipjack

C GOST

D 3DES

B

Which of the following uses a 80 bit key on 64 bit blocks?

A Twofish

B AES

C Skipjack

D DES

C

With _____, the message is divided into blocks and each block is encrypted separately. This is the most basic mode for symmetric encryption.

A Electronic codebook (ECB)

B Cipher-block chaining (CBC)

C Cipher feedback (CFB)

D Output feedback (OFB)

B Electronic codebook (ECB)

C Output feedback (OFB)

D Cipher-block chaining (CBC)

C

Which of the following modes can be used to turn a block cipher into a stream cipher?

A Propagating cipher-block chaining (PCBC) and Electronic codebook (ECB)

B Counter Mode (CTR) and Propagating cipher-block chaining (PCBC)

C Electronic codebook (ECB) and Output feedback (OFB)

D Output feedback (OFB) and Counter Mode (CTR)

D

A fixed-size pseudorandom number that is fed into a symmetric cipher to increase randomness is called what?

A IV

B Key

C Chain

D Salt

A

A number that is used only one time then discarded is called what?

A Nonce

B Chain

C Salt

D IV

A

Which of the following is generally true about block ciphers?

A Secret block ciphers should be trusted.

B Block ciphers permute the bits of the input plaintext.

C The plaintext and ciphertext are always the same size.

D A block cipher is an encryption function for variable-size blocks of data.

C

What does the OCSP protocol provide?

A encryption

B VPN connectivity

C hashing

D a real time protocol for verifying certificates

D

U.S. encryption standard that replaced DES. Block symmetric cipher that uses 128-bit block sizes and various key lengths (128, 192, 256).

AES

DES, 3DES, SHA, AES (some AES implementations are Type I)

Class 3 Algorithms

Encryption method where the sender and receiver use an instance of the same key for encryption and decryption purposes.

organizations for which proof of identity is required

Class 2 Certificates

Block symmetric cipher that uses a 128-bit key and 64-bit block size.

International Data Encryption Algorithm (IDEA)

individuals, and intended for email

Class 1 Certificates

A form of cryptanalysis applicable to symmetric key algorithms that was invented by Eli Biham and Adi Shamir.

The examination of differences in an input and how that affects the resultant difference in the output.

Differential cryptanalysis

Cryptanalysis attack where the attacker is assumed to have access to sets of corresponding plaintext and ciphertext.

Known plaintext attack

Carries out real-time validation of a certificate and reports back to the user whether the certificate is valid, invalid, or unknown.

_____ checks the CRL that is maintained by the CA.

Online Certificate Status Protocol (OCSP)

What is the formula Me%n related to?

Cipher text (C) is equal to the encryption function (E) with the key (k) and plain-text (p) being passed as parameters to that function

C = E(k,p) Symmetric encryption

It is impossible to compress the data such that the code is less than the Shannon entropy of the source, without it being virtually certain that information will be lost

Shannon's source coding theorem

A non-secret binary vector used as the initializing input algorithm for the encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance.

IV (Initialization Vector)

If a cryptanalysis uncovers a method that can derive a key for an algorithm, but is only slightly faster than brute force, what is this called?

Success

- Confidentiality
- Access control
- Integrity
- Authentication
- Nonrepudiation

PKI services

It should be impossible for any attacker to calculate, or guess from an inner state of the generator, any previous numbers in the sequence or any previous inner generator states

BSI criteria K4 states:

The result of these two steps yields a _____.

Digital Signature

A 16-round Feistel cipher working on 64-bit blocks. Unlike DES, it can have varying key sizes ranging from 32 bits to 448 bits. Designed by Bruce Schneier.

Blowfish

Which of the following modes can be used to turn a block cipher into a stream cipher?

Output feedback (OFB) and Counter Mode (CTR)

Online business transactions between companies

Class 4 certificates

_____ is encryption for files while _____ is used for full disk encryption

EFS vs. Bitlocker

Cryptanalysis attack that exploits vulnerabilities within the algorithm structure.

Analytic attack

Open-community and standardized version of SSL

but _____ is more extensible and is backward compatible with SSL.

Transport-Layer Security (TLS)

Uses a block size of 128 bits and key sizes up to 256 bits. It is a Feistel cipher. Designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson.

Twofish

160 bit hash

SHA-1

Cryptographic attack that exploits the mathematics behind the birthday problem in the probability theory forces collisions within hashing functions.

Birthday attack

A process that puts a message into the least significant bits of a binary file is called what?

Steganography

Cryptanalysis attack that tries to uncover a mathematical problem from two different ends.

Meet-in-the-middle attack

Asymmetric encryption method developed in 1984. It is used in PGP implementations and GNU Privacy Guard Software. Consists of 3 parts: key generator, encryption algorithm, and decryption algorithm.

El Gamal

A combination of the ISAKMP and OAKLEY protocols.

Internet Key Exchange (IKE)

The payload of the message is protected

Transport mode

A protocol for online shopping with a credit card. One of its features is that it encrypts the credit card number so that an eavesdropper cannot copy it.

SET

_____ is the worst enemy of security, and it almost always comes in the form of features or options.

Complexity

_____ is a measure of how many things interact at any one point. If the effect of an option is limited to a small part of the program, then it cannot interact with an option whose effect is limited to another part of the program.

Complexity

The original message, m is called the _____

plaintext

The public-key algorithms are used to establish _____, which in turn is used to encrypt the actual data. This combines the flexibility of public-key cryptography with the efficiency of symmetric-key cryptography.

a secret key

Digital signatures are the public-key equivalent of _____.

message authentication codes

This is a proposed hash function standard still in development. This is being chosen in a public review process from non-government designers. An ongoing NIST hash function competition is scheduled to end with the selection of a winning function, which will be given the name _____ in 2012.

SHA-3

This hash function uses 512-bit blocks and implements preset constants that change after each repetition. Each block is hashed into a 256-bit block through four branches that divides each 512 block into sixteen 32-bit words that are further encrypted and rearranged. Because the four branches are used in parallel, whereas SHA-256 uses four serial rounds, _____ is hard to analyze.

FORK-256

_____ is a 160-bit hash algorithm developed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel. There exist 128-, 256-, and 320-bit versions of this algorithm, called RIPEMD-128, RIPEMD-256, and RIPEMD-320, respectively. These all replace the original RIPEMD which was found to have collision issues. The larger bit sizes make this far more secure that MD5 or RIPEMD.

RACE Integrity Primitives Evaluation Message Digest (RIPEMD-160)

The input message is broken into 512-byte chunks (16-32 bit integers).

The message is padded with zeros if needed to reach 512-byte chunks.

The length of the message (before padding) is then appended as the last 64 bits of the message.

The algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C, and D. They are initialized to an initial variable.

The algorithm consists of four stages or rounds, each of which consists of 16 similar operations.

Those operations are a non-linear function F, a modular operation, and a shift.

The MD5 Algorithm

This hash algorithm was initially defined in the Russian national standard and produces a fixed-length output of 256 bits. The input message is broken up into chunks of 256-bit blocks. If a block is less than 256 bits, then the message is padded by appending as many zeros to it as are required to bring the length of the message up to 256 bits. The remaining bits are filled up with a 256-bit integer

arithmetic sum of all previously hashed blocks and then a 256-bit integer representing the length of the original message, in bits, is produced.

GOST

This hash function was designed by Ross Anderson and Eli Biham in 1995 and is 192 bits. It is designed using the Merkle-Damgård construction (sometimes call the Merkle-Damgård paradigm). This is a method to build collision-resistant cryptographic hash functions from collision-resistant one-way compression functions. The Merkle-Damgård construction was described in Ralph Merkle's Ph.D. dissertation in 1979.

TIGER

An _____ adds a key to a hash to improve integrity.

HMAC or Hash Message Authentication Code

A _____, uses a block cipher in CBC mode to improve integrity.

MAC or Message Authentication Code

In PKI, Bob encrypts the message with Alice's _____ and sends it. When Alice receives the message, they can decrypt it with her _____.

public key; private key

In information theory,_____ is a measure of the uncertainty associated with a random variable.

entropy

Related to entropy, _____ states: it is impossible to compress the data such that the code rate is less than the Shannon entropy of the source, without it being virtually certain that information will be lost.

Cryptographic Modules

FIPS 186 covers what?

Digital Signatures

FIPS 197 covers what?

AES

Table look-up

Hardware

Algorithmic (software)

The 3 Types of Generators

FIPS 201 covers what?

Identity Verification

What provides all 3 of the following?

-Authentication

-Integrity

-Non-repudiatio

Good digital signature schemes

A _____ is an entity trusted by one or more users to manage certificates

CA (Certification Authority)

Frequency Analysis

In a _____, the attacker obtains the ciphertexts corresponding to a set of plaintexts. This can allow the attacker to attempt to derive the key used and thus decrypt other messages encrypted with that key.

Chosen plaintext attack

A _____ is less effective, but much more likely for the attacker since the attacker only has access to a collection of ciphertexts.

NOTE: The attacker ONLY has access to the ciphertext of messages.

Ciphertext-only attack

The _____ is similar to the chosen-plaintext attack, except the attacker can obtain ciphertexts encrypted under two different keys. (The keys need to be related, meaning that one was derived from the other as is the case in wireless systems)

Related-key attack

A known-plaintext attack and uses a linear approximation to describe the behavior of the block cipher.

Given sufficient pairs of plaintext and corresponding ciphertext, bits of information about the key can be obtained and increased amounts of data will usually give a higher probability of success.

Invented by Mitsarue Matsui.

Linear Cryptanalysis

_____ is a form of cryptanalysis applicable to symmetric key algorithms and was invented by Eli Biham and Adi Shamir.

The 3 resources for cryptanalysis

A one-way mathematical operation that reduces a message or data file into a smaller fixed length output, or hash value.

Variable data input (of any size) + hashing algorithm = fixed bit stream output (hash value)

MD5 = 128 bits

SHA1 = 160 bits

Hash Function

Different encryption keys generate the same ciphertext from the same plaintext message.

Key clustering

The time and effort required to break a protective measure.

Work factor

Each block of plaintext is XORed with the XOR of the previous plaintext block and the previous ciphertext block before being encrypted. As with CBC mode, an initialization vector is used in the first block.

Propagating Cipher Block Chaining (PCBC)

A number that has no factors in common with another number (3 & 7)

Co-prime numbers

Which system of encryption is used to authenticate users on wireless local area networks in a home environment?

A Chacha20

B SHA-256

C A5 stream encryption method

D WPA-PSK

D

a networking device that allows wireless-capable devices to connect to a wired network

wireless access point

one of the earliest security algorithms used for wireless networks to provide data confidentiality

Wired Equivalent Privacy (WEP)

a stream encryption method used on mobile networks

A5 ciphers

Which cryptanalysis attacks involve examining patterns in the random characters combined with the plaintext message to produce the ciphertext to see how long the key goes before it starts to repeat?

A Linear cryptanalysis

B Frequency analysis

C Algebraic attacks

D Keystream analysis

D