WRQ Networking Security Glossary

Compiled by Eric Raisters

Updated: JULY 16, 2002

AES (Advanced Encryption Standard) – NIST recently (2001) completed a selection process for the algorithm to use as the newest U.S. data encryption standard in FIPS 197. The algorithm selected is the Rijndael algorithm, which is a variable block and key-length algorithm. The algorithm was selected in a public competition from five finalists. (See Rijndael)

ARC4 (Arcfour) – This is the purported public-domain implementation of RSA's RC-4 encryption algorithm. All experience to-date has shown that Arcfour is functionally equivalent and interoperable with RSA's clients and servers using RC-4.

Asymmetric Cipher - Where the key to encrypt a message is different from the key used to decrypt the message. An example is a public key cipher.

Attack - General ways in which a "bad guy" may try to penetrate a network security system. These are not algorithms; they are just approaches as a starting place for constructing specific algorithms. Some commonly discussed attacks include:

- **Brute Force** (or Exhaustive Search): Try all possible keys until deciphering yields readable messages.
- **Codebook** (the classic codebreaking approach): somehow get, or guess, some amount of the plaintext, and use it to start a codebook of transformations between plaintext and ciphertext.
- **Known Plaintext**: First assume the presence of some amount of original plaintext and accompanying ciphertext (this is often a very reasonable assumption). Use this information to try and reconstruct the internal state or cipher key.
- **Defined Plaintext**: Submit arbitrary messages to be ciphered and capture the resulting ciphertext, thus disclosing the workings of the cipher.
- **Man-in-the-Middle** (or spoofing): Subvert the routing capabilities of a computer network, and pose as the other side to each of the communicators. Sometimes also called a bucket brigade attack. Normally takes advantage of the generally unrecognized need to validate or certify public keys.
- **Differential Cryptanalysis**: Use any statistical unbalance between different keys, data elements, or bits to imply a probable state internal to the cipher.
- **Social Engineering**: Gather sufficient pieces of information from various staff within an organization to acquire access to a system or network of systems.

Authentication - The process of reliably determining the identity of a communicating party. This can be done with passwords, credentials, certificates, biometrically, etc.

Authorization - Permission to access a specific resource. The authorization information can vary by host, subnet, and username and may or may not be included with the authentication information.

Blowfish - A very fast, public-domain, open-source block encryption algorithm developed by Bruce Schnieier of Counterpane Systems. Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits and works on a 64-bit block.

Break - The result of a successful attack, usually attributed to either codebook, known or defined plaintext, differential cryptanalysis or social engineering attacks. Breaking the cipher destroys the advantage of the entire algorithm and any messages that have been enciphered with that algorithm.

CA (Certification Authority) - An entity (system) that signs certificates and thus vouches for the certificate bearer.

CAST - A symmetric key algorithm similar to DES designed by Carlisle Adams and Stafford Taveres (hence CAST) and patented by Entrust Technologies, but publicly available. The 128-bit algorithm is described in RFC 2144. The 256-bit algorithm has been submitted as a candidate for the NIST Advance Encryption Standard (AES).

CAT (Common Authentication Technology) - A common definition of security service interfaces and protocols and their interoperability as specified in RFC 1511.

CBC (Cipher Block Chaining) - An operating mode for block ciphers. CBC mode is essentially a crude meta-stream cipher which streams block transformations. In CBC mode the ciphertext value of the preceding block is exclusive-OR combined with the plaintext value for the current block. This has the effect of distributing the enciphered plaintext values evenly among all possible block values, and so prevents codebook attacks.

CRL (Certificate Revocation List) - A digitally signed message from the authoritative CA that lists all of the unexpired but revoked certificates issued by the CA. Similar to the book of stolen credit card numbers distributed to stores.

CRC (Cyclical Redundancy Check) - A form of non-cryptographic integrity check popular for error detection. CRC-32 is a 32-bit CRC commonly used in message integrity checking.

Cipher - A secrecy mechanism or process which operates on individual characters or bits independent of semantic content. As opposed to a secret code, which generally operates on words, phrases or sentences, each of which may carry some amount of complete meaning. There are two major taxonomies of ciphers:

- **Block cipher**: A block cipher requires the accumulation of some amount of data or multiple data elements for ciphering to complete. Usually used for file transfer protocols such as FTP.
- **Stream cipher**: A stream cipher has the ability to transform individual elements one-by-one. The actual transformation usually is a block transformation, and may be repeated with the same or different keying. Usually used for short data transfer protocols such as Telnet.

Ciphertext - The result of enciphering. Ciphertext will contain the same information as the original plaintext, but hide the original information, typically under the control of a key. Without the key it should be impractical to recover the original information from the ciphertext.

Code - Symbols or values which stand in place of other symbols or values. Classically, a numeric value might represent a word or entire phrase so as to decrease the cost of telegraph messages. In modern usage, a code is a correspondence between information (such as character symbols) and values (such as the ASCII code). Coding is a very basic part of modern computation and generally implies no secrecy or information hiding. Some codes are "secret codes," however, and then the transformation between the information and the coding is kept secret.

Crack - The result of a successful attack, usually attributed to either brute force or man-in-the-middle attacks. Cracking the code destroys the advantage of a cipher in hiding information usually for only a single message or session.

Credentials - Secret information used to prove one's identity in an authentication exchange.

Cryptanalysis - The process of finding weaknesses or flaws in cryptographic algorithms. That aspect of cryptology which concerns the strength analysis of a cryptographic system, and the penetration or "breaking" of a cryptographic system. Also "codebreaking." A cipher might be considered "broken" when the information in a message can be extracted without needing the specific key for that message. The work involved may be great or small, and may or may not need to be repeated on every message.

Cryptographic checksum - An integrity check with the property that it is infeasible to find a valid checksum for a message unless you know some secret.

Cryptography - Secret writing. The art and science of transforming information into an intermediate form which hides that information. A part of cryptology. As opposed to steganography, which seeks to hide the existence of any message, cryptography

seeks to render a message unintelligible even when the message is completely exposed. Cryptography includes secrecy and authentication.

DASS (Distributed Authentication Security Service) - A public key-based authentication protocol defined in RFC-1507.

DCE (Distributed Computing Environment) - A group of programs and protocols standardized by the Open Software Foundation (OSF) built atop the cryptographically protected remote procedure call (RPC) protocol. Earlier, often seen on OpenVMS, IBM-AIX and HP-UX systems, but now much less prevalent.

Decryption - The general term for extracting information which was hidden by encryption. Syn: decipher.

DES (Data Encryption Standard) - The particular block cipher which is the U.S. Data Encryption Standard as established by NIST in FIPS 46-1. A 64-bit block cipher with a 56-bit key organized as 16 rounds of operations. The DES algorithm has been published and extensively scrutinized for potential weaknesses. It has never been broken, but has been cracked by computerized brute force attack.

Diffie-Hellman key exchange - A method of establishing a shared key over an insecure medium, named after the inventors. The security of Diffie-Hellman relies on the difficulty of the discrete logarithm problem (which is believed to be computationally equivalent to factoring large integers). Diffie-Hellman is claimed to be patented in the United States, but the patent expired April 29, 1997 and some doubt now exists whether the patent was even valid.

DSA (Digitial Signature Algorithm) - A digital signature algorithm defined by NIST.

DSS (Digital Signature Standard) - A public key cryptographic system for computing digital signatures (i.e. it does not do encryption).

Elliptic curve cryptography - Elliptic curve public key cryptography is more complicated, but has the advantage that the public keys and certificates can be much smaller for the same amount of security. Elliptic curve is detailed in IEEE P1363 Draft Standard on Elliptic Curve Cryptosystems and Related Methods.

Encryption - The general term for hiding information in secret code or cipher. Syn encipher.

GSSAPI (Generic Security Service Application Programmers Interface) - a library and a set of C-binding routines that may be used for authentication, integrity checking and encryption as defined in RFCs 1508, 1509 and 2078.

Hash - A classic computer operation which forms a fixed-size result from an arbitrary amount of data. Ideally, even the smallest change to the input data will change

about half of the bits in the result. Often used for table look-up, so that very similar language terms or phrases will be well-distributed throughout the table. Also often used for error-detection, and, known as a message digest authentication.

IDEA (International Data Encryption Algorithm) **-** The secret key block cipher used in PGP. Designed by James Massey and Xuejia Lai in several installments, called PES, IPES and IDEA. IDEA is patented in Europe and the US by Ascom-Tech AG. It is round-based, with a 64-bit block size, a 128-bit key, and no internal tables.

Kerberos - A DES-based authentication system developed at MIT as part of project Athena and subsequently incorporated into a growing collection of commercial products (including Microsoft's Windows 2000 and XP). Kerberos assumes that the systems themselves can be secured (KDC and application servers) but the network between them is insecure. It is specified in IETF RFC 1510.

Key - A quantity used in cryptography to encrypt and decrypt information.

KDC (Key Distribution Center) - An on-line trusted intermediary that has master keys for all principals and which generates conversation keys between principals when requested. Usually associated with Kerberos.

Key Distribution Problem - The problem of distributing keys to both ends of a communication path, especially in the case of secret key ciphers, since secret keys must be transported and held in absolute secrecy. Also refers to the problem of distributing vast numbers of keys, if each user is given a separate key. Although this problem is supposedly "solved" by the advent of the public key cipher, in fact, the necessary public key validation is almost as difficult as the original problem. Although public keys can be exposed, they must represent who they claim to represent, or a "spoofer" or man-in-the-middle can operate undetected.

MAC (Message Authentication Code) - A synonym for Message Integrity Check (MIC).

MARS - A fixed-block, variable key-length encryption algorithm developed by IBM Research and one of the five AES finalists. It supports key lengths from 128 to over 400-bits. This algorithm is available with a worldwide, royalty-free license from Tivoli.

MD-2™ - A proprietary (to RSA) message digest function that is a one-pass algorithm that produces a 128-bit digest.

MD-4™ - A proprietary (to RSA) message digest function that is a three-pass algorithm that produces a 128-bit digest.

MD-5™ - A proprietary (to RSA) message digest function that is a four-pass algorithm that produces a 128-bit digest.

Message Digest - A small value that represents an entire message for purposes of authentication; a hash. Commonly used hashes include MD-2, MD-4 and MD-5 (defined in RFCs 1319, 1320 and 1321, respectively) as well as CRC-32.

MIC (Message Integrity Check) - A fixed length quantity generated cryptographically and associated with a message to reassure the recipient that the message is genuine. This term is most often used in connection with secret key cryptography, since a public key MIC is more commonly called a digital signature.

Mutual authentication - When each party in a conversation proves its identity to the other.

NIST (National Institute of Standards and Technology) - The US government body that proposes and sets standards. Formerly known as the National Bureau of Standards.

PGP (Pretty Good Privacy) - A popular public key cipher system using both RSA and IDEA ciphers. RSA is used to transfer a random key; IDEA is used to actually protect the message. One problem with PGP is a relatively unworkable facility for authenticating public keys. While the users can compare a cryptographic hash of a key, this requires communication through a different channel, which is more than most users are willing to do. The result is a system that generally supports man-in-the-middle attacks, and these do not require "breaking" either of the ciphers.

PKCS (Public-Key Cryptography System) - a series of documents produced and distributed by RSA Data Security (a Security Dynamics company), proposing techniques for using public key cryptographic algorithms in a safe and interoperable manner. Defined in IEEE P1363 and RSA's PKCS #1, #3, #5, #6, #7, #8, #9 and #10.

PKI (Public Key Infrastructure) also PKIX - An IETF working force tasked with developing Internet standards needed to support an X.509-based PKI. The goal of this PKI will be to facilitate the use of X.509 certificates in multiple applications that make use of the Internet and to promote interoperability between different implementations choosing to make use of X.509 certificates. The resulting PKI is intended to provide a framework which will support a range of trust/hierarchy environments and a range of usage environments Candidate applications to be served by this PKI include, but are not limited to, PEM, MOSS, GSS-API mechanisms (e.g., SPKM), ipsec protocols, Internet payment protocols, and www protocols.

Plaintext - Plaintext is the original, readable message. It is convenient to think of plaintext as being actual language characters, but may be any other symbols or values (such as arbitrary computer data) that need to be protected.

Preauthentication - A protocol for proving you know your password before you are allowed to access a high quality secret encrypted with that password. In Kerberos, preauthentication prevents any plaintext messages to be sent during the authentication procedure.

Principal - A completely generic term used by the security community to include both people and computer systems and the services they provide.

Public Key Cipher - Also called an asymmetric cipher. A type of cipher which uses one key to encipher a message, and a different key to decipher the resulting ciphertext. This allows the enciphering key to be exposed, without exposing the message. As opposed to a secret key cipher. Either key can be used for enciphering or deciphering. Usually the exposed key is called the "public" key, and the retained hidden key is called the "private" key. A public key cipher is vastly slower than a secret key cipher, and so is normally used simply to deliver the message key or session key for a conventional or secret key cipher.

Although first proclaimed as a solution to the key distribution problem, it soon became apparent that someone could pretend to be someone else, and send out a "spoofed" public key. The spoofer could then receive the message, decipher and read it, then re-encipher and send it to the correct destination. Note that spoofing can penetrate cipher security without breaking either the public key cipher or the internal data cipher. Thus, the simple use of a public key cipher which cannot be broken (assuming the private key is kept secret) is not sufficient to guarantee security.

To prevent spoofing, public keys must be "validated" or "certified" as representing who they claim to represent. This can be almost as difficult as the conventional key distribution problem. Since a secret key cipher has no complex key distribution protocol, the simple use of a secret key cipher which cannot be broken (assuming the secret key is kept secret), is sufficient to guarantee security.

RC-2™ - A proprietary (to RSA) secret key block encryption scheme with 64-bit blocks and varying key length. Named after its inventor, Ron Rivest, the acronym stands for Rivest's Cipher #2.

RC-4™ - Another proprietary (patented by RSA) secret key stream algorithm that effectively produces an unbounded length pseudorandom stream from a varying key length. Common key lengths are 40 and 128-bit. Named after its inventor, Ron Rivest, the acronym stands for Rivest's Cipher #4. This algorithm is the most commonly used one for secure web transactions.

RC-5™ – The latest proprietary (patented by RSA) secret key stream algorithm with variable block size, key length and number of rounds. Supports key lengths from 0- to 2048-bits. Named after its inventor, Ron Rivest, the acronym stands for Rivest's Cipher #5.

RC-6™ – A public, symmetric, block algorithm based in RC-5 in that uses data rotation, but with the use of multiplication instead of addition or XOR operations. Supports variable key lengths up to 1024-bits. Named after its inventor, Ron Rivest, the acronym stands for Rivest's Cipher #6.

Rijndael – A public, iterated variable key- and block-length encryption algorithm developed by Joan Daemen and Vincent Rijmen of the University of Leuwen in Belgium and based on the SQUARE algorithm design. Supports key lengths of 128-, 192- and 256-bits. It was recently (fall, 2001) selected as the new U.S. Advanced Encryption Standard (AES) algorithm in a public competition from five finalists.

Realm - A Kerberos term for all of the principals served by a particular KDC.

RSA™ - The name of an algorithm published by Ron Rivest, Adi Shamir, and Len Adleman (thus, R.S.A.). The first major public key system. Based on number-theoretic concepts and using huge numerical values, a RSA key must be perhaps ten times or more as long as a secret key for similar security. The RSA cryptographic algorithms are trademarked and patented, and so licensing and royalty fees must be paid to RSA Data Security (a Security Dynamics company) for use. Many of the US patents expired in the year 2000. Since the RSA algorithm is proprietary and has not been publicly scrutinized, it is unknown whether it can be broken or cracked, or if it might contain back-door access.

SERPENT - A fixed-block, variable key-length encryption algorithm developed by Ross Anderson (Univ. of Cambridge, UK), Eli Biham (Technion Univ., Israel) and Lars Knudsen (Technical Institute of Bergen, Norway). It was one of the five AES finalists. It supports key lengths of 128-, 192- and 256-bits.

SET™ (Secure Electronic Transfer) - A specification designed to utilize technology for authenticating the parties involved in payment card purchases on any type of online network, including the Internet. SET was developed by Visa and MasterCard and uses digital certificates for authentication.

SHA (Secure Hash Algorithm) - A message digest function proposed by the NIST in FIPS 183.

SHS (Secure Hash Standard) - Another message digest function proposed by the NIST. This one is a five-pass function that produces a 160-bit hash. Usually referred to as SHA-1.

S-HTTP (Secure Hypertext Transfer Protocol) - A protocol for providing more security for WWW transactions. In many ways it is more flexible than SSL.

Signature - A quantity associated with a message which only someone with knowledge of your private key could have generated, but which can be verified through knowledge of your public key.

SKIPJACK - A secret key encryption algorithm using 64-bit blocks and 80-bit keys. It is embedded in Clipper chips and has now been de-classified by the US government.

SOCKS - A TCP proxy across firewalls protocol developed by NEC for client/server environments. SOCKS includes two primary components, the SOCKS server and the SOCKS client library. The SOCKS server implementation is at the application layer and the SOCKS client library is between the client's application and transport layers. Technically, it is referred to as a Circuit-Level Gateway, meaning that it proxies virtual circuit connections so that both the application client and the server believe they are connected to each other in the next layer, the application layer. The SOCKS V4 protocol performs three functions; connection request, proxy circuit setup, and application data relay. The SOCKS V5 protocol adds authentication and data encryption.

ssh™ (Secure Shell) - A protocol that provides support for secure remote login, secure file transfer, and secure TCP/IP and X11 forwardings. It can automatically encrypt, authenticate, and compress transmitted data. SSH is developed by SSH Communications Security Ltd. in Finland and the name “ssh” is trademarked.

SSH2 - A protocol that is used to secure terminal sessions and arbitrary TCP-connections. SSH2-protocol is based on SSH1-protocol, developed by Tatu Ylönen. This is an evolving standard protocol being worked on by the Secure Shell working group of the IETF.

Steganography - Covered writing. Methods of cryptology which seek to conceal the existence of a message. As opposed to cryptography which seeks to hide the information in the message, even if the message itself is completely exposed.

Strength - The ability of a cipher to resist attack and maintain secrecy. Although "strength" would seem to be the entire point of using a cipher, cryptography has no way to measure strength. Nobody really knows what "strength" is. As far as we know, "strength" is a negative, the lack of any attack. Normally, cipher strength is discussed in the context of particular attacks, but these may or may not represent the actual threat to the cipher in the field.

SSL (Secure Sockets Layer) - A secure communications protocol developed by Netscape to provide authentication via public key, message integrity checking via SHA or MD5 and encryption with RC4 or DES algorithms. Current version is 3.1.

SSLeay - Started by Eric Young as an effort to implement the SSL protocol, but has since turned into a fairly complete freeware cryptographic library called OpenSSL. Used in the open- source Apache web server.

Symmetric Cipher (or shared secret) - Where the key to encrypt a message is also used to decrypt the message. An example is Kerberos.

Ticket - A data structure constructed by a trusted intermediary to enable two parties to authenticate.

TLS (Transport Layer Security) - The new name for the next generation SSL protocol which is currently continuing to be defined as a public standard in RFC 2246. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP), is the TLS Record Protocol which provides connection security. Above that the TLS Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. Current version is 1.0 and does not, by default, interoperate with SSL 3.x although a backward compatibility mechanism is incorporated into the standard.

TGT (Ticket Granting Ticket) - A Kerberos data structure which is a ticket to the KDC.

Triple DES (3DES) - The particular block cipher which is the U.S. Data Encryption Standard for DES, with two or three different keys. The 56-bit algorithm is used three times in sequence, usually encrypting with first 56-bit key, decrypting with the second 56-bit key and encrypting with the either a last or the first 56-bit key.

Twofish – A public domain, open-source fixed-block encryption algorithm developed by Bruce Schneier of Counterpane Systems that was one of the five AES finalists. It supports keys of 128-, 192- and 256-bits.

VPN (Virtual Private Network) - A client/server security system that allows for the creation of an encrypted tunnel between the client and a server inside of an enterprise's firewall. The client-side piece is usually a shim in the stack. Ideally VPN's are protocol and application independent.

X.400 - A CCITT (a European telecommunications standards organization now called ITU) standard for electronic mail.

X.500 - A CCITT standard for directory services.

X.509 - A CCITT standard for security services within the X.500 directory services framework. The X.509 encoding of public key certificates has been widely adopted with version 3 being the current level. Described in RFC 1422.

Resources for this glossary:

Ritter's Crypto Glossary by Terry Ritter: http://www.io.com/~ritter

Network Security: Private Communication in a Public World by Charlie Kaufman, Radia Perlman, Mike Speciner. PTR Prentice Hall, 1995. ISBN 0-13-061466-1