Glossary

A

A5/1 - a stream cipher that makes use of linear feedback shift registers.

Abelian Group - a group S is called Abelian if for any a, b in S, a * b = b * a.

Active Attack - an attack in which the attacker modifies messages being communicated.

Advanced Encryption Standard (AES) - a block cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, as a submission to a competition to replace DES.

AKS Primality Test - a deterministic primality test that can be performed in polynomial time.

Associative - operator * is associative if for a, b, c we have a * (b * c) = (a * b) * c .

Asymmetric (Public Key) Cryptography - form of cryptography that uses a public/private key pair: one for encryption and the other for decryption

Asynchronous Stream Cipher - astream cipher in which the keystream depends on the ciphertext.

Authentication - confirmation to the receiver of a message that the data received has been sent only by an identified and verified sender.

Authentication Process - procedure used in verifying digital signatures.

Availability - ensuring that information can be accessed and modified only by authorised users in an appropriate time-frame.

Avalanche Effect - a desirable property of cryptographic algorithms where if an input is changed slightly (for example, flipping a single bit), the output changes significantly (e.g., half the output bits flip).

B

Baby-Step Giant-Step Algorithm - an algorithm used to speed up trial multiplication in calculating discrete logarithms.

Berlekamp-Massey Algorithm - an algorithm that will find the shortest linear feedback shift register for a given binary output sequence.

Bigram - a pair of consecutive letters, often used in frequency analysis.

Birthday Paradox - the probability that, in a set of n randomly chosen people, some pair of them will have the same birthday.

Bit Commitment Protocol - a protocol that allows someone to commit to a chosen value while keeping it hidden to others, with the ability to reveal the committed value later.

Bitcoin - a decentralized digital currency without a central bank or single administrator that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.

Bitcoin Address - the address to which bitcoins are registered, which is the hash of the public key.

Blind - the random value used in digital signatures.

Blind Signature - a digital signature where where the signatory is able to sign a document without seeing its content, thereby ensuring sender privacy.

Block Cipher - a symmetric cipher that encrypts one fixed size block of data at a time.

Block Replay Attack - an attack on block cipher in which a previously transmitted ciphertext block is inserted into a new communication.

Blockchain - a growing list of records, called blocks, that are linked using cryptography.

Blowfish - a block cipher developed by Bruce Schneier with 16 rounds, a 64-bit block and variable key length from 1 to 448 bits..

Blum Blum Shub Generator - an iterative cryptographically secure pseudo-random number generator.

Bombe - a mechanical device built at Bletchley Park to emulate the Enigma machine.

Brute Force Attack - an attack in which the attacker tries to determine the key by attempting all possible keys.

C

Caesar Cipher - a historical cipher which is a shift cipher with a shift value of 3.

Carmichael Number - a composite number that is always determined to be probably prime using the Fermat primality test.

CBC-MAC - a message authentication code (MAC) based on block ciphers in CBC mode.

Central Authority - a trusted entity that can be used to distribute and authenticate keys in cryptography

Certificate Authority (CA) - an entity that issues digital certificates.

Certificate Revocation List (CRL) - a blacklist of cancelled certificates which must not be trusted.

Chaining - a technique used in block ciphers where the encryption of a block is dependent on its context.

Characteristic - the XOR difference between two plaintexts, used in differential cryptanalysis.

Chinese Remainder Theorem (CRT) - a result that allows us to replace a modular computation using a large composite modulus with smaller more efficient computations using the factors of the modulus instead.

Chosen Ciphertext Attack - an attack in which the attacker chooses the ciphertext and can obtain its decryption.

Chosen Plaintext Attack - an attack in which the attacker chooses the plaintext to be encrypted, so has the ciphertext-plaintext pair of their choice.

Cipher - an algorithm for performing encryption and decryption

Cipher Block Chaining (CBC) - one of the modes of operation of block ciphers in which the previous ciphertext block is fed into the encryption of the current block.

Cipher Feedback (CFB) - one of the modes of operation of block ciphers in which the previous ciphertext block is fed into the encryption of the current block.

Ciphertext - an encrypted message

Ciphertext Only Attack - an attack in which the attacker has access to a set of ciphertexts, but does not have access to the corresponding plaintexts.

Collision - for hash functions, a situation where two different inputs result in the same digest.

Collision Free - a required property of hash functions that means that it should be difficult to find two different inputs that result in the same digest.

Commutative Group - another name for an Abelian group.

Commutative - operator * is commutative if for a, b we have a * b = b * a.

Composite Number - an integer that has more than two factors.

Compression Function - another name for a hash function.

Computational Security - a cryptographic system is called computationally secure if the best possible algorithm for breaking it is computationally infeasible.

Confidentiality - keeping information hidden from those who are not entitled or authorised to see it.

Confusion - an important property for a block cipher where there is a non-linear relationship between the plaintext and the ciphertext.

Congruent Modulo n - a is congruent to b modulo n if a and b have the same remainder when divided by n.

Coprime - another name for relatively prime.

Counter (CTR) - one of the modes of operation of block ciphers in which a counter is used to ensure that the same plaintext block will not always be encrypted to the same ciphertext block.

Crib - a common phrase which is the likely plaintext corresponding to a ciphertext.

Cryptanalysis - the analysis and deciphering of secret writings.

Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) - a pseudo-random number generator for which it is not possible to predict the next number given the previous numbers in the sequence.

Cryptography - the act or art of writing in secret characters.

Cryptology - the scientific study of cryptography and cryptanalysis.

Cryptosystem - a suite of cryptographic algorithms needed to implement a particular security service

Cut and Choose - a protocol used in verifying digital coins.

Cyclic Redundancy Check (CRC) - a checksum used for error detection in transmitted data.

D

Data Encryption Standard (DES) - a block cipher developed in the early 1970s by IBM as a submission to a contest to select a government-approved block cipher.

Decisional Diffie-Hellman Problem (DDH) - a hard problem related to the Diffie-Hellman problem

Decryption - method for decoding messages.

Deep Crack - a machine built by the Electronic Frontier Foundation (EFF) in 1998, to perform a brute force search of the DES keyspace.

Dictionary Attack - an attack in which the attacker builds a table of ciphertexts and corresponding plaintexts that they have learnt over a period of time.

Differential Cryptanalysis - a chosen plaintext cryptanalytic attack where differences in inputs are mapped to differences in outputs.

Differential Fault Analysis (DFA) - a side channel attack to investigate ciphers and extract keys by generating faults in a system that is in the possession of the attacker, or by natural errors that occur.

Differential Power Analysis (DPA) - a side channel attack that consists not only of visual but also statistical analysis and error-correction statistical methods to obtain information about the keys.

Diffie-Hellman Key Exchange - an algorithm for two entities to establish a shared symmetric key.

Diffie-Hellman Problem (DHP) - the hard problem that has to be solved to break the Diffie-Hellman key exchange protocol.

Diffusion - an important property for a block cipher where each bit of the ciphertext depends on many bits of the plaintext.

Digest - the fixed length output from a hash function.

Digital Certificate - an electronic document used to prove the ownership of a public key.

Digital Signature - a mathematical scheme for verifying the authenticity of digital messages or documents

Digital Signature Algorithm (DSA) - a digital signature scheme used in the Digital Signature Standard.

Discrete Logarithm - given p, g and g^a (mod p), determine a.

Discrete Logarithm Problem (DLP) - the difficult mathematical problem of determining to which power some value was raised in order to obtain the result in modular arithmetic.

Dividend - a number to be divided by another number.

Division Theorem - if a is an integer and n a positive integer, then there are unique integers q and r, with $0 \leq r < n$, such that $a = n \times q + r$.

Divisor - a number by which another number is to be divided.

E

Electronic Code Book (ECB) - one of the modes of operation of block ciphers in which the same plaintext block is always encrypted to the same ciphertext block.

Elgamal Encryption - a public key encryption scheme, the security of which rests on the difficulty of the Diffie-Hellman problem.

Elgamal Signature - a digital signature scheme proposed by Taher Elgamal.

Encryption - method for encoding messages.

End-to-End Encryption - a truly secure messaging system where only the sender and receiver can read the message.

Enigma Machine - a mechanical rotor device used by the German for encryption during World War 2.

Enity Authentication - assurance that data has been received from a specific entity, say a particular website.

Euclidean Algorithm - an algorithm to compute the greatest common divisor of two integers.

Euler Group - a set of invertible elements in modular arithmetic.

Euler Liar - a composite number determined to be probably prime using the Solovay-Strassen primality test.

Euler Pseudoprime - a number determined to be a probable prime using the Solovay-Strassen primality test.

Euler Witness - a number determined to be definitely prime using the Solovay-Strassen primality test.

Euler's Criterion - a criterion that is used to determine whether a number is a quadratic residue with respect to a prime modulus.

Euler's Theorem - a corollary of Lagrange's theorem that can be used to simplify the calculation of modular exponentiation.

Euler's Totient Function - a function for determining the number of elements in a Euler group.

Exclusive Or (XOR) - a logical operation that outputs 1 when the inputs are different, and 0 otherwise.

Extended Euclidean Algorithm (XGCD) - an extension of the Euclidean algorithm for computing the greatest common divisor of two integers that can be used for computing multiplicative inverses.

F

Factor - an integer that evenly divides a number without leaving a remainder.

Factor Base - the set of prime numbers less than a smoothness bound.

Factorisation - the decomposition of a composite number into its prime factors.

Fast data Encipherment ALgorithm (FEAL) - a block cipher proposed as an alternative to DES, and designed to be much faster in software, but susceptible to various forms of cryptanalysis.

Feedback Function - a function applied to the set of cells that are 'tapped' in a feedback shift register.

Feedback Shift Register - a small circuit containing a number of memory cells, each of which holds one bit of information and often used to construct stream ciphers.

Feistel Cipher - a symmetric structure used in the construction of block ciphers

Fermat Liar - a composite number determined to be probably prime using the Fermat primality test.

Fermat Primality Test - a probabilistic test making use of Fermat's little theorem to determine whether an integer is probably prime.

Fermat Pseudoprime - a number determined to be a probable prime using the Fermat primality test.

Fermat Witness - a number determined to be definitely prime using the Fermat primality test.

Fermat's Factorisation Algorithm - an algorithm for integer factorisation, devised by Fermat.

Fermat's Little Theorem - a special case of Lagrange's theorem that can be used to determine probable primes.

Field - a set of elements with two binary operators that must satisfy additional properties to those of a ring.

Finite Field - a field with a finite number of elements.

Finite Group - a group with a finite number of elements.

Frequency Analysis Attack - an attack in which the attacker uses the frequency of occurrence of letters in the underlying language to crack the ciphertext.

Fresh Key - a recently created key not used by any other party before.

Fundamental Theorem of Arithmetic - this states that every positive number can be represented as a product of primes in a unique way, up to a permutation of the order of primes.

G

Galois Field - another name for a finite field.

Great Internet Mersenne Prime Search (GIMPS) - a collaborative project of volunteers who use freely available software to search for Mersenne prime numbers.

Greatest Common Divisor (GCD) - the greatest common divisor of integers a and b is the largest integer that evenly divides both a and b.

Group - a set of elements with a binary operator that must satisfy certain properties.

Group Theory - the study of groups.

H

Hash Function - a mathematical function that converts a binary string of arbitrary length into another short binary string of fixed length.

Hash Value - the fixed length output from a hash function.

Hash-Based Message Authentication Code (HMAC) - a type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key.

I

Index - another name for a discrete logarithm.

Information Theoretic Security - another name for unconditional security.

Initialisation Vector (IV) - a random initial value used in many modes of operation in block ciphers.

Integer Factorisation - the decomposition of a composite number into a product of smaller prime factors.

Integer Factorisation Problem (IFP) - the difficult mathematical problem of decomposing a composite number into a product of smaller prime factors.

Integrity - ensuring that data is accurate and trustworthy.

International Data Encryption Algorithm (IDEA) - a sufficiently strong block cipher with a block size of 64 and a key size of 128 bits.

Irreducible Polynomial - a polynomial that cannot be expressed as a product of two polynomials of lower degree.

Iterated Cipher - a cipher in which a simple encryption function is applied iteratively a number of times.

J

Jacobi's Symbol - a value that is used to determine whether a number is a quadratic non-residue with respect to a composite modulus.

K

Key Distribution Problem - the problem of distributing symmetric keys, which quickly becomes difficult to manage for larger numbers of users.

Key Pair - the public and private key that are mathematically linked to each other in public key cryptography.

Key Schedule - the algorithm used to derive the round keys in an iterated cipher from the cipher key.

Key Whitening - a technique intended to increase the security of an iterated block cipher by combining the data with portions of the key.

Keystream - a pseudo-random sequence used in stream ciphers and effectively replaces the long key that is used in the one-time pad.

Known Plaintext Attack - an attack in which the attacker knows the plaintext for some parts of the ciphertext.

L

Lagrange's Theorem - a theorem that can be used to simplify the calculation of modular exponentiation.

Legendre's Symbol - a value that is used to determine whether a number is a quadratic residue with respect to a prime modulus.

Linear Complexity - the size of the shortest program that can be used to produce a keystream

Linear Congrentual Generator - an iterative pseudo-random number generator

Linear Cryptanalysis - a known plaintext cryptanalytic attack where the aim is to find linear approximations to the action of a cipher.

Linear Feedback Shift Register(LFSR) - a feedback shift register in which the feedback function is a linear function of the tapped bits.

Lucas-Lehmer Primality Test - a deterministic primality test that makes use of Mersenne primes.

Lucifer - the name given to several of the earliest block ciphers, developed by Horst Feistel and his colleagues at IBM.

M

Man in the Middle Attack - an attack in which the attacker inserts themselves in between the communication between two participants.

Manipulation Detection Code (MDC) - a way for the receiver of a message to ensure the integrity of the message by making use of a hash function.

Meet in the Middle Attack - a space–time tradeoff cryptographic attack against encryption schemes which rely on performing multiple encryption operations in sequence.

Merkle-Damgård Construction - a method of building collision-resistant cryptographic hash functions from collision-resistant one-way compression functions.

Mersenne Number - an integer that is one less than a power of 2 (for powers above 1).

Mersenne Prime - a Mersenne number that is a prime.

Message Authentication - confirmation to the receiver of a message that the data received has been sent only by an identified sender.

Message Authentication Code (MAC) - a way for the receiver of a message to ensure its integrity and that the message was sent by an identified sender by making use of a hash function with a key.

Message Digest (MD) - a family of hash functions that includes MD2, MD4, MD5 and MD6.

Miller-Rabin Primality Test - a probabilistic test making use of Fermat's little theorem to determine whether an integer is probably prime.

Mining - the process of adding transactions to the blockchain.

Modes of Operation - the different ways in which block ciphers can operate in terms of using the encryption of previous blocks to affect the further encryption of blocks.

Modular Arithmetic - a system of arithmetic for integers, where numbers wrap around upon reaching a certain value (the modulus).

Modular Exponentiation - repeated multiplication of a number by itself in modular arithmetic.

Modular Square Root - the square root of a quadratic residue in modular arithmetic.

Modulus - the remainder after division of one number by another.

Monoalphabetic Substitution Cipher - a substitution cipher in which all occurrences of a letter in the plaintext are replaced with the same letter in the ciphertext.

Multiplicative Inverse - the multiplicative inverse of x is a number which, when multiplied by x, yields the multiplicative identity, 1.

N

Next-Bit Test - a test for cryptographically secure pseudo-random number generators that requires that given the first k bits of a random sequence there is no efficient algorithm that offers a greater than 50% probability of correctly predicting bit k+1 of the sequence.

Non-Linear Feedback Shift Register(NLFSR) - a feedback shift register in which the feedback function is a non-linear function of the tapped bits.

Non-Malleable - the property of a cipher where on seeing the ciphertext resulting from encrypting a message, it is impossible to determine a valid ciphertext on a related message.

Non-Repudiation - assurance that the original creator of a message cannot deny the creation or transmission of the message to a recipient or third party.

Nonce - a random number used only once that can be used to ensure freshness.

Number Field Sieve - a method for integer factorisation devised by John Pollard.

O

One-Time Pad (OTP) - an encryption technique that cannot be cracked if used correctly.

One-Way Function - a function f for which it is easy to compute y = f(x), but given y it is computationally infeasible to invert the function to compute x.

Optimal Asymmetric Encryption Padding (OAEP) - a padding scheme often used together with RSA encryption.

Oracle - an efficient algorithm to solve a problem.

Order - the order of a group S, denoted by |S|, is the number of elements in S.

Output Feedback (OFB) - one of the modes of operation of block ciphers in which the previous cipher output is fed into the encryption of the current block.

P

P-Box - a permutation box, often used to provide diffusion in a block cipher.

Padding - extra bits added to the end of a message in a block cipher to make it up to a multiple of the block length.

Passive Attack - an attack in which the attacker eavesdrops on communication, but does not modify it in any way.

Perfect Security - another name for unconditional security.

Period - in a generated sequence of pseudo-random numbers, the period is the number of these that are generated before the sequence repeats.

Plaintext - an unencrypted message (in the clear).

Plaintext Aware - the property of a cipher where it is computationally difficult to construct a valid ciphertext without knowing the corresponding plaintext to start with

Pollard lambda Method - a method for computing discrete logarithms devised by John Pollard.

Pollard p-1 Method - a method for integer factorisation devised by John Pollard.

Pollard rho Method - a method for integer factorisation devised by John Pollard. Also the name of a method for computing discrete logarithms devised by John Pollard.

Polyalphabetic Substitution Cipher - a substitution cipher in which occurrences of the same letter in the plaintext are replaced with different letters in the ciphertext.

Polynomial Ring - polynomial ring F[x] is the set of all polynomials over variable x with coefficients in the field F.

Polytime Reduction - the reduction of one problem to another in polynomial time.

Post-Quantum Cryptography - cryptosystems that are secure from attack by quantum computers.

Pre-Image Resistant - a required property of hash functions that means that given an input and its digest, it should be hard to find a different input with the same digest.

Pretty Good Privacy (PGP) - an encryption program that provides cryptographic privacy and authentication for data communication.

Primality Test - a test used to determine whether an integer is prime.

Prime Factorisation - the dividing of an integer into its prime factors.

Prime Number - an integer that is only divisible by 1 and itself.

Prime Number Theorem - this states that the number of primes less than X is approximately X/log X.

Primitive Root - a number that can be used to generate an Euler group when raised to successive powers.

Private Key - the secret key in asymmetric cryptography that can be used to decrypt confidential messages and create digital signatures.

Proof of Work - a proof of someone having committed a large amount of resources to a problem, to provide trust in blockchain transaction verification.

Provably Secure - a cryptographic system is provably secure if breaking the system would be equivalent to solving some well-studied hard problem that cannot currently be solved within a reasonable period of time.

Pseudo-Hadamard Transform (PHT) - a reversible transformation of a bit string that provides cryptographic diffusion.

Pseudo-Random Number Generator - an algorithm that can create long runs of numbers with excellent random properties but eventually the sequence repeats.

Public Key - the publicly available key in asymmetric cryptography that can be used to encrypt confidential messages or verify digital signatures.

Public Key Infrastructure (PKI) - a set of roles, policies, and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

Purple Machine - a Japanese encryption device built as a modification of the Enigma Machine.

Q

Quadratic Non-Residue - a number that cannot be the result of a squaring operation in modular arithmetic.

Quadratic Residue - the result of squaring a number in modular arithmetic.

Quadratic Residuosity Problem (QUADRES) - the hard problem of determining whether a number is a quadratic residue modulo a composite number.

Quotient - a result obtained by dividing one number by another.

R

Rabin Encryption - a public key encryption scheme, the security of which rests on the difficulty of the modular square root problem.

RACE Integrity Primitives Evaluation Message Digest (RIPEMD) - a family of hash functions that includes RIPEMD, RIPEMD-128 and RIPEMD-160.

Random Seed - the initial input value to a pseudo-random number generator.

Randomisation - the adding of a random value to messages.

RC4 - a stream cipher designed by Ron Rivest in 1987.

RC5 - an iterated block cipher designed by Ronald Rivest in 1994 with a variable block size (32, 64 or 128 bits), key size (0 to 2040 bits) and number of rounds (0 to 255).

Reciprocal - another name for the multiplicative inverse.

Reduction - the reduction of one problem to another by showing one problem can be used to solve the other.

Redundancy - the adding of redundant data to a message.

Relatively Prime - two integers are relatively prime if there is no integer greater than one that divides them both, so their greatest common divisor is one.

Remainder - the integer left over after dividing one integer by another.

Replay Attack - an attack in which the attacker captures every piece of traffic between two entities during normal operation and later replays it.

Rijndael - the original name of the AES block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen

Ring - a set of elements with two binary operators that must satisfy certain properties.

Root CA - the certification authority (CA) at the top level in the CA hierarchy.

Round Function - the simple encryption function applied in each iteration of an iterated cipher.

Round Key - the key for a particular round of an iterated cipher, derived from the cipher key.

RSA - the first published method for implementing public key cryptography invented by Ron Rivest, Adi Shamir and Leonard Adleman.

RSA Problem (RSAP) - the hard problem that has to be solved to break the RSA public-key encryption scheme.

S

S-Box - a substitution box, often used to provide confusion in a block cipher.

Safe Prime - if p is a prime, p-1 = 2q and q is a prime, then q is called a safe prime.

Salt - a known random value that is combined with a password before applying the hash and is stored alongside the hash in the password file.

Second Pre-Image Resistant - a required property of hash functions that they should be computationally infeasible to reverse.

Secret Splitting - a method for distributing a secret.

Secure and Fast Encryption Routine (SAFER) - a family of block ciphers designed primarily by James Massey (one of the designers of IDEA).

Secure Hash Algorithm (SHA) - a family of hash functions that comprises SHA-0, SHA-1, SHA-2 and SHA-3.

Secure Socket Layer (SSL) - a cryptographic protocol designed to provide communications security over a computer network.

Security Protocol - a sequence of steps that performs a security-related function using cryptographic methods.

Semantic Security - the property of a cipher where it does not reveal any information about the message being encrypted.

Sequence Number - sequential number associated with messages to prove they are fresh.

Session Key - a single-use symmetric key used for encrypting all messages in one communication session.

Shift Cipher - a cipher in which each plaintext letter is replaced with a different one at a fixed number of places down the alphabet.

Shor's Algorithm - a quantum computer algorithm for integer factorisation discovered by Peter Shor. This algorithm can also be modified to compute discrete logarithms.

Side Channel Attack - an attack in which the attacker tries to exploit any weakness in the physical implementation of the cryptosystem.

Side Channel Cryptanalysis - a cryptanalytic attack to exploit a weakness in the physical implementation of a cryptosystem.

Sieve of Eratosthenes - an inefficient method for finding prime numbers.

Signing Protocol - protocol used in performing digital signatures

Simple Power Analysis (SPA) - a side channel attack based on looking at the visual representation of the power consumption of a unit while an encryption operation is being performed.

Simple Substitution Cipher - a monoalphabetic substitution cipher in which all occurrences of a letter in the plaintext are replaced with the same letter in the ciphertext.

Smart Contract - a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract.

Smooth Number - an integer that factors completely into small prime numbers.

Smoothness Bound - a bound on the size of prime factors.

Solovay-Strassen Primality Test - a probabilistic test making use of Euler's criterion to determine whether an integer is probably prime.

Square and Multiply Algorithm - an efficient algorithm for performing modular exponentiation.

Square Root Problem (SQROOT) - the hard problem of determining the modular square root with a composite modulus.

State Compromise Extension - a problem with pseudo-random number generators where knowledge of the state of the number generating process makes it possible to reconstruct the stream of pseudo-random numbers already generated, thus showing that the pseudo-random number generator is not secure.

Stream Cipher - a symmetric cipher that encrypts an arbitrary stream of bits or bytes.

Strong Liar - a composite number determined to be probably prime using the Solovay-Strassen primality test.

Strong Pseudoprime - a number determined to be a probable prime using the Solovay-Strassen primality test.

Strong Witness - a number determined to be definitely prime using the Solovay-Strassen primality test.

Subkey - the key for a particular round of an iterated cipher, derived from the cipher key.

Substitution-Permutation Network (SPN) - a type of iterated block cipher that applies several alternating rounds consisting of a substitution layer followed by a permutation layer to produce each block of ciphertext.

Symmetric Cryptography - form of cryptography that uses a single key to encrypt the plaintext to ciphertext and also to decrypt the ciphertext back into plaintext.

Synchronous Stream Cipher - a stream cipher in which the keystream depends only on the key.

T

Timestamp - a clock time associated with a message to show that it is fresh.

Timing Attack - a side channel attack based on measuring the time it takes for a unit to perform operations.

Tiny Encryption Algorithm (TEA) - a block cipher designed by David Wheeler and Roger Needham notable for its simplicity of description and implementation, typically a few lines of code.

Tonelli-Shanks Algorithm - a probabilistic algorithm that can be used to determine the modular square root of a number if the modulus is congruent to 1 (mod 8).

Transport Layer Security (TLS) - a cryptographic protocol designed to provide communications security over a computer network.

Trapdoor One-Way Function - a one-way function where, given some extra information (the trapdoor information), it is easy to invert the function.

Trial Division - an inefficient method for finding prime numbers or the factors of a composite number.

Trial Multiplication - an inefficient method for computing discrete logarithms.

Trigram - three consecutive letters, often used in frequency analysis.

Triple-DES (3DES) - a block cipher that applies the DES cipher algorithm three times to each data block.

Trivium - a stream cipher that makes use of non-linear feedback shift registers.

Trusted Third Party (TTP) - a trusted entity other than the two main participants in a communication.

U

Unconditional Security - a cryptographic system is said to be unconditionally secure when we place no limit on the computational power of the adversary.

V

Venona Project - a US counterintelligence program initiated during World War II.

Vernam Cipher - another name for the one-time pad.

Vigenère Cipher - an early example of a polyalphabetic substitution cipher that was originally thought to be unbreakable.

W

Weak Key - a key, which, used with a specific cipher, makes the cipher behave in some undesirable way.

Wi-Fi Protected Access (WPA) - a security protocol to secure wireless computer networks.

Wired Equivalent Privacy (WEP) - a security algorithm for IEEE 802.11 wireless networks.