Terms used in the disciplines of
Cryptography, IT Security and Risk Analysis

Access Control v. Grab the mouse.

Act of God n. Don’t try suing us without a repudiation from God.

Affine Cipher n. A terrific encryption algorithm.

Annualised Loss n. Corporation tax.

Asset n. Diminutive posterior. See BACKUP.

Authentication n. Certified as originating from India.

Autokey n. Ignition key.

Backup n. or v. Method of protecting Asset.

BAN Logic v. First rule of brainstorming.

Baseline Control n. Low calorie diet.

Biometric n. Unit of measure for biorhythm.

Birthday Problem n. Present dilemma. May be solved by smart card.

Bit Commitment a. Promise of a small acting part in a movie, perhaps in exchange for sexual favours. May be waived on denial of service (q.v.).

Block Cipher v.t. Policy of outlawing encryption.

BlowFish n. Preference for beef.

Business Continuity n. Weekend work.

Chinese Remainder Theorem n. The belief that the world will be eventually be populated by Orientals.

Cipher v.t. Yearn for.

Ciphertext n. Euphemism for garbage.
Cold Standby, *n.i.* Ability to avoid work by faking a sneeze.

**Code** *n.* Convention, e.g. *code of conduct* or *code of practice*.

**Codebook** *n.* e.g. *Menezes, van Oorschot and Vanstone*, or *Schneier*.

**Codebreaker** *n.* One who behaves badly or never practices.

**Collision** *n.* Different inputs but same outcome, hence . . .

**Collision Resistance** *n.* Reaction against the growing tendency for supposedly different parties to produce similar legislation.

**Confidentiality** *n.* Feeling of confidence (e.g. that data has not been disclosed).

**Control** *n.* Calmness in the face of disaster.

**Copyright** *v.i.* What a good photocopier is supposed to do.

**Countermeasure** *v.t.* The number of bits in a register.

**Cryptanalysis** *n.* Freudian therapy carried out covertly. Hence *Cryptanalyst* *n.*.

**Cryptography** *n.* The art of sneaking snapshots without being observed.

**Decrypt** *n & v.t.* The basement of a Jamaican church.

**Denial of Service** *n.* See *BIT COMMITMENT*.

**DES**. *n. Abbr.* Cryptographic algorithm with key size chosen so that it can be *Decrypted Easily* by Security agencies.

**Dictionary Attack** *n.* Act of throwing the book at a security violator.

**Digital Signature** *n.* Thumbprint.

**Disaster Recovery** *n.* Escape retribution by precipitating a diversionary emergency.

**Discrete Log** *n.* Covert record.

**Eavesdrop** *v.t.* Escape discovery by leaping from upstairs window.

**Email** *a.* Halfway between mail and femail.
Encipher v.t. A way of flagging confidential material so that it can be easily detected by a spell checker. See CIPHERTEXT.

End-to-End Security n. see IT SECURITY.

Error Extension n. Result of confusing aspirin with Viagra.

Exclusive-OR n. Geisha.

Extreme Cipher n. see STREAM CIPHER.

Facsimile n. Good copy. c.f. Facs Differente.

FEAL n. Encryption algorithm. After initial publication, comments on the ease of breaking it led to a series of improvements. Hence Found Easy, Altered Later.

Fingerprint n. Early form of Digital Signature (q.v.). Esp. thumbprint.

Frequency Hopping v.i. Avoiding creditors by never staying long at the same address.

Hash function n. The use of marijuana to reduce problems to manageable size.

Hot Standby n. Spare telephone number in case date does not show up.

Insider a. & n. Marinated in fermented apple juice.

Insurance n. Incriminating photos, letters etc.

Integrity a. Tending to occur in whole numbers rather than fractions.

Internet n. Entrepreneur’s profit after tax.


IT n. Sex.

IT Security n. Safe sex.

Key a. Important.

Key Exchange. n. NYSE.

Key Management n. Senior executives.
**Keystream** *n.* Major waterway, e.g. the Amazon.

**Known Ciphertext Attack** *n.* Easier than Unknown Ciphertext Attack.

**Known Plaintext Attack** *n.* Faking the ability to break a cipher when one already knows the answer.

**Law of Large Numbers** *n.* The theory that Microsoft will finally take over the planet.

**Law of Small Numbers** *n.* Wishful thinking by no-hope minorities.

**Law of Medium-Sized Numbers** *n.* Can we move on please.

**MAC** *n.* 1. Disguise, e.g. for security officer. 2. Term of uninvited familiarity.

**Meet in the Middle** *v.i.* Plan for covert rendezvous.

**Message Digest** *v.t.* What happens after swallowing a secret message.

**Minimum Disclosure Proof** *n.* The principle that the less you say, the less you’ll need to lie about later.

**Network** *n.* 1. Difference between work charged for and work done. 2. Final check before embarking on fishing trip.

**Nonce** *n.* Number, *N* used once. Hence *N*twice, *N*thrice, etc. If *N* is prime it is a *Ponce*.

**Normal Distribution** *n.* In which the tax man gets his cut.

**Notary** *a.* Remarkable.

**NP-Hard** *a.* Non-Pharmacologically hard, *i.e.* not just due to Viagra.

**Number** *a.* More than merely numb, but less than numbest.

**One Time Pad** *n.* Former place of residence (See also **TWO TIME PAD**).

**Password** *n.* Label stuck to a VDU containing date of birth, car registration number, maiden name, etc.

**PC Security** *n.* Name of agency hiring out services of retired Police Constables.

**PIN** *n.* Security mechanism with applications to credit cards and hand grenades.
**Plaintext** *n.* Strong language.

**Protocol** *n.* Soap, with countless scriptwriters, endlessly played out by Alice and Bob.

**Provably Secure** *a.* Can only be broken by cheating.

**Public Key** *n.* Key on a piece of string where anyone can reach it. See also **SESSION KEY**.

**Random Number** *n.* Seventeen.

**Redundancy** *a.* Decruitment.

**Risk Analysis** *v.i.* Take a chance on a course of therapy.

**Risk Management** *v.i.* Take a chance admitting a mistake to senior executive.

**RSA** *n.* *Abbr.* Really Secure Algorithm.

**Secret** *n.* & *a.* See **TOP SECRET**.

**Secret Key** *n.* A key, hidden under a rock.

**Secret-Sharing** *n.* Oxymoron, like **Live Recording**.

**Security** *n.* 1. Mythological state of perfection, Heaven, Nirvana, Cloud Cuckoo Land, etc. 2. Ability to prove that whatever goes wrong is not your fault.

**Security Breeches** *n.* Belt and braces.

**Security Policy** *n.* Insurance certificate.

**Session Key** *n.* Door key of a local bar.

**Smart Card** *n.* Humorous birthday greeting.

**Smooth Number** *n.* Cool outfit.

**Square-Free** *n.* Deserted piazza.

**Standard** *n.* Any one from large range of published specifications, giving a wide choice.

**Standby** *v.* Avoid helping.

**Steganography** *n.* The science of hiding simple ideas in fancy-sounding words.
Stream Cipher n. Mild cipher; see also EXTREME CIPHER.

Strict Avalanche Criterion n. Restrictive clause in ski-insurance policy.

Strong Cipher n. Cipher devised by oneself.

Symmetric vs. Asymmetric Cipher n. "cipher" is Asymmetric whereas "ciphpic" is Symmetric.

System n.or a. Word appended to description to increase perceived importance.


Traffic Analysis n. Course of therapy while commuting.

Trapdoor n. & v.t. Term of abuse describing ciphers designed by other people, esp. government agencies.

Trusted Kernel n. Senior army officer with hernia support.

Two Time Pad 1. n. Economically used One Time Pad. (q.v.). 2. n. Venue for covert amorous liaison.

Turing Machine n. Harley Davidson.

Unbreakable a. Term used to describe any new cipher or protocol, or one devised by oneself.

Unicity n. Trivial case of the travelling salesman problem.

Universal Hash Functions n. Trading name of importer of illegal substances.

UPS n. Abbr. Well known package delivery agency.

Virus n. Self-replicating, damaging software fragment, proving that if something is stupid enough, but possible, someone will do it.

Watermark n. Residue of keystream (q.v.).

Weak Cipher n. Cipher devised by someone else.

Week Key n. Change it after seven days.
**Wiretap** *v.i.* Economise on water.

**Worm** *n.* Limbless invertebrate.

**Zero-Defect** *n.* Philosophy opposite to Risk Analysis, childlike-belief in possibility of never making mistakes.

**Zero-Knowledge Argument** *n.* 1 The principle of not allowing ignorance of possible damage to future generations to be a barrier to business. 2. Statements like "Two plus two equals five, at least for large values of two".

**Zero-Knowledge Proof** *n.* Rigorous demonstration that a rival is not just incompetent but ignorant.

© John Gordon, Concept Labs 1998. (john@ConceptLabs.co.uk)