The University of Adelaide

AUTO–ID LABS

Definition of Terms used by the Auto-ID Labs in the Anti-Counterfeiting White Paper Series

Alfio R. Grasso and Peter H. Cole

Auto-ID Labs White Paper WP-HARDWARE-024

Mr. Alfio R. Grasso
Deputy Director, Auto-ID Lab, ADELAIDE
School of Electrical and Electronics
Engineering,
The University of Adelaide

Prof. Peter H. Cole
Research Director, Auto-ID Lab, ADELAIDE
School of Electrical and Electronics
Engineering,
The University of Adelaide

Contact:
alf@eleceng.adelaide.edu.au or cole@eleceng.adelaide.edu.au.

Internet: www.autoidlabs.org

ABSTRACT

The objective of this paper is to provide a reference source for terms used by the Auto-ID Labs, in the Anti-Counterfeiting White Paper Series. Such terms are commonly used in the security industry, and are now starting to find their way into RFID applications. While the terms are well defined in the security industry, RFID Engineers need to have a common understanding. Papers in the white series have been reviewed, and when a term is used that is not contained either within ISO 19762 - Harmonized vocabulary, for RFID related terms, or EPCglobal’s Tag/Reader Security Glossary (26th April 2006), a definition is provided in this document.

Appendix A lists useful Security & Authentication Glossaries, available online, some of which have been used to compile this Glossary.

All seven Auto-ID Laboratories contributed in some way to the definition of terms. Many of the definitions in this document have come from Wikipedia (http://en.wikipedia.org/), and are licensed under the GNU Free Documentation License.

1.1. AES:

Advanced Encryption Standard (AES) was announced in September 1997as the successor to DES. AES is a Federal Information Processing Standard (FIPS), specifically, FIPS Publication 197 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf), that specifies a cryptographic algorithm for use by U.S. Government organizations to protect sensitive, unclassified information. AES supports key sizes of 128 bits, 192 bits, and 256 bits, in contrast to the 56-bit keys offered by DES. The reference for this description is http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html.

1.2. Abelian Group:

In mathematics, an abelian group, also called a commutative group, is a group (G,*), such that a*b=b*a for all a and b in G. In other words, the order of elements under the conjunction * doesn't matter.

1.3. Annihilating Polynomial:

If R is a quotient polynomial ring, then f in R is called an annihilating polynomial if the norm value of f is zero, i.e., || f || = 0. || ° || indicates centred-norm, see Centred Norm below.

1.4. Anti-cloning:

Anti-cloning as applied to RFID is when the RFID tag has a property such that it cannot be cloned (duplicated) without affecting the original.

1.5. Asymmetric Public Key System:

An asymmetric public key system is a cryptographic system in which a different key is used to decrypt a message from the key originally used to encrypt the message. RSA is an example of an asymmetric public key system. Each user has a public key, which is different for each user, which is exchanged via secure methods such as digital signatures, trusted systems or otherwise. Each user also has a private key, again which is different for each user. The public and private keys are mathematically related, but to deduce (calculate) the private key from the public is believed to be extremely difficult (it has not yet been mathematically proven). See also Cryptography / Cryptographic Algorithm, Public Key Cryptography Systems, Public/Private Keys, RSA and Symmetric Key System definitions below.

1.6. Authentication:

Authentication is the act of establishing or confirming something (or someone) as authentic, that is that claims made by or about the thing are true. Authenticating an object may mean confirming its provenance, whereas authenticating a person often consists of verifying their identity. Authentication depends upon one or more authentication factors.

1.7. Back-end Server :

In their most general meanings, the terms front end and back end refer to the initial and the end stages of a process flow. As applied to RFID and software applications running on host computers, the front-end is responsible for collecting input from the user (reading EPC tags) and processing it in such a way that it conforms to a specification that the back-end can use. The front-end is the part of a software system that interacts directly with the user, and the back-end comprises the components such as a database that process the output from the front-end. Back-end system usually takes the form of a middleware, database management, application server, and derives sensible and related information from tag’s raw data (obtained from the front end RFID readers).

1.8. Basis:

A basis B of a vector space V is a linearly independent subset of V that spans V

1.9. Basis – Short:

A basis {(f, g), (F, G)} is called a short basis in NTRU lattice L_h^{NT} if

$$\| f \|, \| g \| = O(\sqrt{N}), \text{ and } \| F \|, \| G \| = O(N).$$

Where,

f and g are binary polynomials

Small polynomials (F, G) satisfy $f * G - g * F = q$, and q: is a modulus.

1.10. Basis – Longer:

The security of NTRUSign scheme is based on the approximately closest vector problem in a certain lattice, called NTRU lattice. In this scheme, the signer can sign a message by demonstrating the ability to solve the approximately closest vector problem reasonably well for the point generated from a hashed message in a given space. For example, the signer's private key is a short basis for an NTRU lattice and his public key is a much longer basis for the same lattice. See Basis - Short above.

1.11. Biometrics:

The study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioural traits.

1.12. Bio-Metric Data:

Distinct data of one or more measurable, physical or behavioural characteristic of a person which is used to recognise the identity or verify the claimed identity.

1.13. Brute Force Attack:

A brute force attack is a method of defeating a cryptographic scheme by trying a large number of possibilities; for example, exhaustively working through all possible keys in order to decrypt a message. In most schemes, the theoretical possibility of a brute force attack is recognised, but it is set up in such a way that it would be computationally infeasible to carry out. Accordingly, one definition of "breaking" a cryptographic scheme is to find a method faster than a brute force attack. The selection of an appropriate key length depends on the practical feasibility of performing a brute force attack. By obfuscating the data to be encoded, brute force attacks are made less effective as it is more difficult to determine when one has succeeded in breaking the code.

1.14. Buffer Overflow Vulnerability:

In computer security and programming, a buffer overflow, or buffer overrun, is an anomalous condition where a process attempts to store data beyond the boundaries of a buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data. Buffer overflows may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits. Sufficient bounds checking by either the programmer or the compiler can prevent buffer overflows. See Heap Smashing Attack and Stack Smashing Attack below.

1.15. Centred Norm:

The NTRUSign algorithm uses the centred norm concept instead of Euclidean norm in verification step to measure the size of an element a ε R. If a(x) is a polynomial in ring R, where R=Z[x]/(x^N-1), then the centred norm of a(x) is denoted by

$$\| \, a(x) \, \|^2 = \textstyle\sum_{i=0}^{N-1}(a_i - \mu_a)^2 = \sum_{i=0}^{N-1} {a_i}^2 - \frac{1}{N}(\sum_{i=0}^{N-1} a_i)^2,$$

where $\mu_a = \frac{1}{N} \sum_{i=0}^{N-1} a_i$ is the average of the coefficients of $a(x)$.

1.16. Certification:

A certificate is an official document affirming some fact. In computing and especially computer security and cryptography, the word certificate generally refers to a digital identity certificate, also known as a public key certificate.

1.17. Challenge-and-Response Protocol:

The Challenge-Response protocol is an exchange of information used to establish the authenticity of a party in a communication session. It is a common authentication technique in which one party presents a question ("challenge") and another party must provide a valid answer ("response") to be authenticated. It allows for the comparison of private data ("a key") without the need to transfer the private information over a possibly unsecured channel

One example, among many varieties of challenge and response mechanisms, is as follows: the sender chooses a challenge x, which is a random number and transmits it to the receiver. The receiver computes y = eK (x) and transmits the value y to the reader (here e is the encryption rule that is publicly known and K is a secret key known only to the sender and receiver). The receiver then computes y’ = eK (x) and then verifies that y’ = y.

1.18. Characteristic polynomial :

The characteristic polynomial of a linear feedback shift register is defined as the polynomial $P_n(x) = 1+ c_1x + c_2x^2 + \ldots +c_nx^n$, with $c_n \neq 0$, and where the feedback coefficients c_i of the register are either 0 or 1. The characteristic polynomial is primitive if (a) it has no proper factors and (b) $P_n(x)$ does not divide x^d+1 for any $d<2^n-1$.

1.19. Chosen Message Attack (Chosen Plaintext Attack):

A chosen message (or plaintext) attack is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which reduces the security of the encryption scheme. In the worst case, a chosen plaintext attack could reveal the scheme's secret key.

1.20. Ciphertext:

Ciphertext is the message after the original message (or plaintext) has been encrypted.

Ciphertext = Encryption(plaintext). See keystream and plaintext below.

1.21. Clandestine Scanning:

Clandestine Scanning is the reading the content of a RFID tag without the consent and possibly without the knowledge of the holder of the tag.

1.22. Clandestine Tracking:

Clandestine Tracking is the tracking of an RFID tag without the consent and possibly without the knowledge of the holder of the tag. Tracking can be conducted through clandestine scanning, though it is possible also even if the data on the chip cannot be read.

1.23. Cloning of a Tag (Clone):

Cloning is the production of a tag with identical properties of a certain (legitimate) tag. Normally only digital properties (e.g. EPC, transponder ID number, PIN code, secret keys etc.) are considered.

1.24. Cloning Resistance:

Cloning Resistance is the property of a tag that defines the amount of effort that has to be expended in order to clone the tag. It can consist of a combination of logical obstacles (e.g. breaking of an encrypted message) and physical obstacles (e.g. reading a certain part of the tag memory).

1.25. Closest Vector Problem:

There are two famous computational problems on lattices: the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP).

In SVP, one is given a basis b_1; b_2; …… ; b_n and must find the shortest non-zero vector in $L(b_1; b_2; ……; b_n)$.

In CVP, one is given a basis b_1; b_2; ……; b_n and a target vector v (not necessarily in the lattice) and must find the lattice vector in L(b_1; b_2;……; b_n) closest to v.

The problem of the closest lattice vectors in the l2-norm is

$$CVP \quad := \quad \left\{ (k,m,n,b_1,\cdots,b_n,z) \;\middle|\; \begin{array}{c} k,m,n \in \mathbb{N}, b_1, b_2, \cdots, b_n, z \in \mathbb{Z}^m, \\ \exists x \in L(b_1, b_2, \cdots, b_n) \\ : \parallel z - x \parallel^2 \leq k \end{array} \right\}$$

Given a lattice basis b_1; b_2; ……; b_n ε Z^m, the following tasks are thought to be hard algorithmic lattice problems:

- Find a short non-trivial lattice vector.
- Find a basis comprised of short lattice vectors.
- Find for a given z ε span(b_1; b_2; …… ; b_n) the closest lattice vector.

1.26. Code Injection Vulnerability:

Code injection is a technique to introduce (or "inject") code into a computer program or system by taking advantage of the un-enforced and unchecked assumptions the system makes about its inputs. Most of these problems are related to erroneous or no assumptions of what input data is possible, or the effects of special data. The purpose of the injected code is typically to bypass or modify the originally intended functionality of the program. Classic examples of dangerous assumptions a software developer might make about the input to a program include:

- assuming that metacharacters for an API never occurs in an input; e.g. assuming punctuation like quotation marks or semi-colons would never appear;
- assuming only numeric characters will be entered as input;
- assuming the input will never exceed a certain size;
- assuming that numeric values are equal or less than upper bound;
- assuming that numeric values are equal or greater than lower bound;
- assuming that client supplied values set by server (such as hidden form fields or cookies), cannot be modified by client. This assumption ignores known attacks such as Cookie poisoning, in which values are set arbitrarily by malicious clients;
- assuming that it is okay to pick pointers or array indexes from input;

- assuming an input would never provide false information about itself or related values, such as the size of a file.

1.27. Computationally intractable:

Computationally intractable problems are mathematical problems that are solvable in theory, but cannot be solved in practice. What can be solved "in practice" is open to debate, but in general only problems that have polynomial-time solutions are solvable for more than the smallest inputs.

To see why exponential-time solutions are not usable in practice, consider a problem that requires 2^n operations to solve (n is the size of the input). For a relatively small input size of n=100, and assuming a computer that can perform 10^{10} (10 giga) operations per second, a solution would take about $4*10_{12}$ years, much longer than the current age of the universe.

1.28. Cookie:

A cookie is a string of data exchanged between a web server and a web browser that may contain user preferences and personal information. Cookies are assigned to a web browser during the protocol negotiation. When the same web browser accesses that particular domain again, it constructs its request header such that it contains the cookie information, provided that cookies have been enabled in the web browser and that the cookie has not expired.

1.29. Counterfeit Attack:

This is when an adversary is able to respond to legitimate reader communication and provide (duplicate) the corresponding response signal of a valid tag. This is normally used to introduce fake or illegitimate goods into the supply chain.

1.30. Cover-Coding:

Cover-coding is a technique for obscuring the data that is transmitted over an insecure link, to reduce the risks of snooping. An example of cover-coding would be for the sender to perform a bitwise XOR (exclusive OR) of the original data with a password or random number which is known to both sender and receiver. The resulting cover-coded data is then transmitted from sender to the receiver, who uncovers the original data by performing a further bitwise XOR (exclusive OR) operation on the received data using the same password or random number.

1.31. Cryptography / Cryptographic Algorithm:

A Cryptographic Algorithm is firmware or some combination of hardware, software and firmware that implements cryptographic logic or processes, on a data input stream and transforms the data to render its meaning unintelligible (i.e., to hide its semantic content), prevent its undetected alteration, or prevent its unauthorized use. If the transformation is reversible, cryptography also deals with restoring encrypted data to intelligible form.

Cryptography systems can be broadly classified into:

- Symmetric-key systems that use a single key that both the encryptor and decryptor have, and
- Asymmetric-key (Public-key) systems that use two keys, a public key known to everyone and a private key that only the decryptor or the signer of the message uses. The public key is generally used for encryption and/or Digital Signature verification.

1.32. Cryptography Engine:

The term Cryptography Engine refers to a device which is able to perform cryptography related computations.

1.33. Data Keys (KD):

Data keys are used for bulk encryption, and are used in a three level key management system (ANSI X9.17), used in financial institutions. The highest level is Master Key, which is the most secure and manually delivered, some Master Keys are one-time codes. The next level is a Key Encryption Keys (KEK), which are encrypted from the Master Key, and used by major nodes in the financial network to establish a local secure connection, and are changed periodically. Data keys are the lowest level and used to encrypt message.

1.34. Data Theft:

Data theft is the act of stealing of data from a system's data repository. This can enable cloning of tags in a way that does not concern the tag's cloning resistance, for example if it is used to acquire all digital properties of a tag.

1.35. Decryption/ Encryption:

A cryptographic transformation of encrypted data that restores encrypted data to its original state.

1.36. Denial of Service (DoS) Attack:

A denial-of-service attack (also, DoS attack) is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

1.37. DES:

Data Encryption Standard (DES) is the name of the Federal Information Processing Standard (FIPS) 46-3, which describes the data encryption algorithm (DEA). The DEA is also defined in the ANSI standard X3.92. The DEA has a 64-bit block size and uses a 56-bit key during execution (8 parity bits are stripped off from the full 64-bit key). The DEA is a symmetric cryptosystem, specifically a 16-round Feistel cipher and was originally designed for implementation in hardware.

When used for communication, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message, or to generate and verify a message authentication code (MAC) (see Message Authentication Code below).

1.38. Diffie-Hellman problem:

The Diffie-Hellman problem (DHP) is the task in cryptography of computing gxy given g, gx, and gy, where g is an element of some group, typically the multiplicative group of a finite field, or an elliptic curve group. In other words, the problem is to perform the private key operation given only their public keys in a Diffie-Hellman key exchange. A fast means of solving the DHP would yield a method to break Diffie-Hellman key exchange and many of its variants. To specify the problem with complete precision, one must specify the group exactly and how x and y are generated. The problem was first posed by Whitfield Diffie and Martin Hellman. In cryptography, for certain groups, it is assumed that the DHP is hard, and this is often called the Diffie-Hellman assumption.

1.39. Digital Signature:

A value (called “digital signature” or simply “signature”) computed with a cryptographic algorithm for a data object in such a way that any one can use the signature to verify the data's originator and integrity. The originator of the data object can be verified if it is enclosed in the data object.

1.40. Distance:

Also known as Centred Norm, see Centred Norm above.

1.41. DNS:

The domain name system (DNS) stores and associates many types of information with domain names, but most importantly, it translates domain names (computer hostnames) to IP addresses. It also lists mail exchange servers accepting e-mail for each domain. In providing a worldwide keyword-based redirection service, DNS is an essential component of contemporary Internet use. Useful for several reasons, the DNS pre-eminently makes it possible to attach easy-to-remember domain names to hard-to-remember IP addresses. In a subsidiary function, the domain name system makes it possible for people to assign authoritative names without needing to communicate with a central registrar each time.

1.42. Eavesdropping:

Eavesdropping is the unauthorized interception of a conversation or data transmission.

1.43. Eavesdropping Attack:

Eavesdropping attack is when an adversary has the ability to conceal themself in the vicinity of a reader-tag communication exchange and listen in the forward channel (Reader to Tag communication) to get the reader-to-tag information. A higher level eavesdropping attack is when an adversary has the ability of detecting the backwards channel (Tag to Reader Communication).

1.44. Electronic Pedigree:

An electronic pedigree (E-Pedigree) consists of a computer file or collection of data which provides a verifiable chain of custody for a physical object. Electronic pedigrees are used to help detect and prevent the insertion of counterfeit goods or unauthorized parts into the legitimate supply chains.

Electronic pedigree documents usually consist of some core information related to the specific object (which may include such details as a unique identifier or Electronic Product Code (EPC), as well as some immutable characteristics, such as date of manufacture, etc.), which is digitally signed and then appended or encapsulated with additional custody records to record the shipping and receiving to/from each subsequent custodian, each of which digitally signs their additional custody records.

Ideally, an electronic pedigree document should exist for each individual object or package, rather than the batch as a whole – and each subsequent custodian should verify the integrity of each pedigree (including verifying all digital signatures) before signing the pedigree themselves and sending it to the next custodian, ideally before sending the physical goods).

Auto-ID technologies such as barcodes and particularly Radio-Frequency Identification (RFID) are being considered for use with implementations of electronic pedigree because they allow for rapid identification of each physical object received - and therefore make the pedigree-enabled shipping and receiving process much more efficient and less labour-intensive, since electronic pedigree management application programs can then use the unique IDs or EPCs to access the corresponding electronic pedigree data and ensure that the correct processes of verification and signing are being observed - and ensuring that the custodian has one electronic pedigree document for each physical object they handle.

Electronic pedigree initiatives are currently underway in the pharmaceutical sector (as a result of state laws in Florida, California, etc. and enforcement of the USA federal Prescription Drug Marketing Act). Other industry sectors may also adopt this approach, particularly where there are concerns about counterfeit or unauthorized goods or parts entering the legitimate supply chain

1.45. Elliptic Curve Cryptography:

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The elliptic curve function is the perimeter of an ellipse $y^2 = x^3 + ax + b$, where all variables, x, y, and parameters, a, b must be integers. The set of points on such a curve (i.e., all solutions of the equation together with a point at infinity) can be shown to form an abelian group (with the point at infinity as identity element). If the coordinates x and y are chosen from a large finite field, the solutions form a finite abelian group. The discrete logarithm problem on such elliptic curve groups is believed to be more difficult than the corresponding problem in (the multiplicative group of nonzero elements of) the underlying finite field. Thus keys in elliptic curve cryptography can be chosen to be much shorter for a comparable level of security. In ECC use, the solution $y^2 = x^3 + ax + b$ is usually done over a modulo field, e.g. $[y^2 = x^3 + ax + b] \bmod(n)$ where n is a prime number.

1.46. Encryption:

See Decryption and Cryptographic Algorithm above.

1.47. E-Passport: (electronic passport)

An ePassport is a passport with an electronic chip. Typically the role of the chip is to store biometric data of the passport holder. The term is used as a synonym for Biometric Passport.

1.48. Euclidean Norm:

On a vector space, the Euclidean norm is $\| v \| = \sqrt{v \cdot v}$, i.e. the norm of v is the positive square root of the scalar product of v with itself. $\| {}^{o} \|$ indicates centred-norm, see Centred Norm above.

1.49. Feistel cipher:

In cryptography, a Feistel cipher is a block cipher with a particular structure, named after IBM cryptographer Horst Feistel. A large proportion of block ciphers use this scheme, including the Data Encryption Standard (DES). The Feistel structure has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule. Therefore the size of the code or circuitry required to implement such a cipher is nearly halved. Feistel ciphers and similar constructions combine multiple rounds of repeated operations, such as:

* Bit-shuffling (often called permutation boxes or P-boxes);

* Simple non-linear functions (often called substitution boxes or S-boxes);

* Linear mixing (in the sense of modular algebra) using XOR

to produce a function with large amounts of "confusion and diffusion". Bit shuffling creates the diffusion effect, while substitution is used for confusion.

1.50. Forward Security (Forward Untraceability):

Forward security is the property of an RFID security system such that an adversary cannot trace the RFID Tag’s data back through previous events in which the RFID Tag was involved in even if the adversary acquires the secret data stored in the RFID Tag.

1.51. Fractal tail distribution:

A long-tailed or heavy-tailed probability distribution is one that assigns relatively high probabilities to regions far from the mean or median. In the context of Internet Traffic a number of quantities of interest have been shown to have a long-tailed distribution. For example, considering the sizes of files transferred from a web-server, then, to a good degree of accuracy, the distribution is heavy-tailed, that is, there are a large number of small files transferred but, crucially, the number of very large files transferred remains significant.

1.52. Firewall:

In computing, a firewall is a piece of hardware and/or software which functions in a networked environment to prevent some communications forbidden by the security policy. A firewall has the basic task of controlling traffic between different zones of trust. Typical zones of trust include the Internet (a zone with no trust) and an internal network (a zone with high trust). The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle (see Least Privilege Principle below).

1.53. Genus:

In general genus is a term from algebraic geometry. It indicates how many twists or torsions are there in the curve. For example for any conic section, such as the circle, the (actual, geometrical) ellipse, parabola, hyperbola, there are no twists, hence genus is 0. Similarly for other planar figures such as a triangle, the genus is 0. Elliptic curves have genus of 1, while hyperelliptic curves have a genus of 2 or more. In general, The Fermat curve, derived from $x^n + y^n = z^n$, has genus g= (n-1)(n-2)/2.

1.54. GGH Signature Scheme:

The Goldreich-Goldwasser-Halevi (GGH) signature scheme is a digital signature scheme based on solving the close vector problem (CVP) in a lattice (see NTRUEncrypt Lattics below). The signer demonstrates knowledge of a good basis for the lattice by using it to solve CVP on a point representing the message; the verifier uses a bad basis for the same lattice to verify that the signature under consideration is actually a lattice point and is sufficiently close to the message point. GGH signatures form the basis for the NTRUSign signature algorithm (see below).

1.55. Hash:

A hash function H is a function that transforms a message m into a fixed size string denoted as the hash value h. h = H(m) Hashing is a quite common technique used in database applications and cryptography. In cryptography, however, hash functions need to exhibit the following requirements:

- One way: Easy to derive h = H(m) but computationally infeasible to calculate the message m given the hash value h.
- Variable input length: It should be possible to derive h = H(m) independent on the size of m.
- Fixed output length: The hash value should always be of the same length independent of the message m.
- Collision free: Given a message x it should be computationally infeasible to find a message y so that H(x) = H(y).

Hash functions are used as message digests (reduction of large message to a much smaller number of bits) to ensure data integrity and to provide a digital signature.

1.56. Hash Lock Scheme:

Hash Lock Scheme is a cryptographic access control mechanism, which authenticates RFID readers to tags. It was firstly introduced by Stephen Weis in the paper “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems”, LNCS 2008. Each hash-enabled (one-way hash function computing capability) tag in this design will have a portion of memory reserved to store a temporary metaID and the tag itself operates in either a locked or unlocked state. In this scheme, a hash function is used for generating metaID. metaID = Hash(key). To lock a tag, a tag owner stores the hash of a random key as the tag’s metaID. To unlock/access a tag, the reader sends the key to the tag, which verifies whether the metaID equals the Hash(key).

1.57. HAVAL-128:

HAVAL is a cryptographic hash function. HAVAL can produce hashes of different lengths. HAVAL can produce hashes in lengths of 128 bits, 160 bits, 192 bits, 224 bits, and 256 bits. HAVAL also allows users to specify the number of rounds (3, 4, or 5) to be used to generate the hash.

1.58. HMAC:

A keyed-hash message authentication code, or HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any iterative cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA-1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function and on the size and quality of the key.

1.59. Heap Smashing Attacks:

A buffer overflow occurring in the heap data area is referred to as a heap overflow (or Heap Smashing Attack) and is exploitable in a different manner to that of stack-based overflows (See Stack Smashing Attack below). Memory on the heap is dynamically allocated by the application at run-time and typically contains program data. Exploitation is performed by corrupting this data in specific ways to cause the application to overwrite internal structures such as linked list pointers.

1.60. Hologram:

A Hologram is an advanced form of photography that allows an image to be recorded in three dimensions. The so-called "holograms" appearing in identity documents, credit cards, banknotes or expensive merchandise are not true holograms. Their apparent depth comes from stereoscopy. If you turn the "hologram" upside down, the depth of the image is inverted. All depth disappears if you turn the hologram 90° or if you look at it with just an eye. This is not the case with true holograms, which are not based on binocular vision but in the reconstruction of a virtual image. True holograms give the same 3D images when viewed at any angle or with just an eye.

1.61. Holographic Memory:

A Holographic Memory offers a way of storing information at high density inside crystals or photopolymers.

1.62. Hyper-Elliptic Curve Cryptography:

Hyperelliptic curve cryptography is similar to elliptic curve cryptography (ECC) insomuch as the algebraic geometry construct of a hyperelliptic curve with an appropriate group law provides an Abelian group on which to do arithmetic.

Although introduced only 3 years after ECC, not many cryptosystems implement hyperelliptic curves because the implementation of the arithmetic isn't as efficient as with cryptosystems based on elliptic curves or factoring (RSA). Because the arithmetic on hyperelliptic curves is more complicated than that on elliptic curves, a properly implemented cryptosystem based on hyperelliptic curves can be more secure than elliptic curve based cryptosystems that have the same key size.

The hyperelliptic curves used are typically of the sort $y^2 = f(x)$, where the degree of $f(x) = 2g+1$, where g=genus.

1.63. IETF:

The Internet Engineering Task Force (IETF) develops and promotes Internet standards, cooperating closely with the W3C and ISO/IEC standard bodies; and dealing in particular with standards of the TCP/IP and Internet protocol suite. It is an open, all-volunteer standards organization, with no formal membership or membership requirements.

1.64. IETF PKIX:

The IETF's Public-Key Infrastructure (X.509), or PKIX working group. The term X.509 certificate usually refers to the IETF's PKIX Certificate and CRL Profile of the X.509 v3 certificate standard, as specified in RFC 3280, commonly referred to as PKIX for Public Key Infrastructure (X.509).

1.65. Indistinguishability:

Indistinguishability means that values emitted by an RFID Tag must not be discriminated from other RFID Tags.

1.66. Integrity (Data Integrity):

Integrity refers to the fidelity (or absence of distortion) of a particular piece of information. The integrity of a document or message is said to be preserved if the information is exactly as it was originally created by its original author, without any alteration to the meaning by other parties who for example may have been involved in the transmission of the data between its creator and the final recipient, Because Digital Signatures are cryptographically generated based on a message digest or hash of the original information, they provide a ‘tamper-evident seal’ around the information over which the signature applies; the slightest change to the information would result in a radically different hash value – and because only the original author of the data has access to the private key used to generate the digital signature from the hash value, any attempt by a third party to modify the signed data in transit will be evident because either:

1) the decrypted digital signature will not match the hash calculated over the modified data OR

2) the public key to be used to successfully decrypt the digital signature (and obtain a match with the hash value) does not correspond to the original author – but rather the public key of a third party which modified the data – hence the need for certificate authorities to establish chains of trust regarding which public keys belong to which organizations or individuals.

1.67. Interlock Protocol:

The Interlock Protocol is a method that exposes a middle-man attack (see Man in the Middle attack below) who might try to compromise two parties that use anonymous key agreement to secure their conversation. The Interlock protocol works roughly as follows: the sender sends half the encrypted message to the receiver. The receiver uses the senders key and replies with half of response encrypted message. The sender then sends the other half of encrypted message to the receiver, who then sends the remainder of the response encrypted message. The strength of the protocol lies in the fact that half of an encrypted message cannot be decrypted. Thus, if the man-in-the-middle intercepts the first half encrypted message he will be unable to decrypt that first half encrypted message (encrypted using his key) and re-encrypt it using the receivers. He must wait until both halves of the message have been received to read it, and can only succeed in duping one of the parties if he composes a completely new message.

1.68. Internet Key Exchange (IKE) Protocol:

Internet key exchange (IKE) is the protocol used to set up a Security Association in the IPsec protocol suite. IKE is defined in RFC 2409 (http://rfc.net/rfc2409.html) and uses a Diffie-Hellman key exchange to set up a shared session secret, from which cryptographic keys are derived. Public key techniques or, alternatively, a Pre-shared key, is used to mutually authenticate the communicating parties.

1.69. Internet Protocol Security (IPsec):

IPsec (IP security) is a standard for securing Internet Protocol (IP) communications by encrypting and/or authenticating all IP packets. IPsec provides security at the network layer. IPsec is a set of cryptographic protocols for (1) securing packet flows and (2) key exchange. There are two secure packet flows (1) Encapsulating Security Payload (ESP) provides authentication, data confidentiality and message integrity; (2) Authentication Header (AH) provides authentication and message integrity, but does not offer confidentiality. Currently only one key exchange protocol is defined, the IKE (Internet Key Exchange) protocol. IPsec protocols operate at the network layer, layer 3 of the OSI model. Other Internet security protocols in widespread use, such as SSL and TLS, operate from the transport layer up (OSI layers 4 - 7). This makes IPsec more flexible, as it can be used for protecting both TCP and UDP-based protocols, but increases its complexity and processing overhead, as it cannot rely on TCP (layer 4 OSI model) to manage reliability and fragmentation.

1.70. Invasive Attacks:

An adversary may simply reverse engineer labels to create fraudulent labels for cloning or DOS attacks or use probing techniques to obtain information stored in memory (micro-probing and Focus Ion Beam editing) or alter information stored in memory (using a laser cutting microscope). Attacks, such as optical probing and fault injection attacks where the chip is removed from its packaging with the passivation layer still unbroken are also invasive attacks but these attacks are may be further qualified as semi-invasive attacks. (See non-invasive attacks below).

1.71. Key Encrypting Keys (KEK):

See Data Keys above.

1.72. Keystream:

A set of bits randomly obtained, in which plaintext can be converted to ciphertext. The most common form of conversion is a process of XORing each bit of the plaintext message with the corresponding bit in the key or keystream.

1.73. Lattice:

(see NTRUEncrypt Lattice below).

1.74. Least Privilege Principle:

In computer science the principle of minimal privilege, also known as principle of least privilege or just least privilege, requires that in a particular abstraction layer of a computing environment every module (which can be for example, a process, a user or a program) must be able to see only such information and resources that are immediately necessary. The idea of the principle is to grant just the minimum possible privileges to permit a legitimate action, in order to enhance protection of data and functionality from faults (fault tolerance) and malicious behaviour (computer security).

1.75. Lightweight Cryptography:

Lightweight cryptography employs symmetric encryption algorithms and modes of encryption, along with key-management schemes, so that implementations can be simplified, to the point that they may be implemented on passive RFID tags, where energy consumption cannot be devoted to intense computational tasks.

1.76. Linear Feedback Shift Register:

A linear feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state. The only linear functions of single bits are xor and inverse-xor; thus it is a shift register whose input bit is driven by the exclusive-or (xor) of some bits of the overall shift register value. The initial value of the LFSR is called the seed, and because the operation of the register is deterministic, the sequence of values produced by the register is completely determined by its current (or previous) state. Likewise, because the register has a finite number of possible states, it must eventually enter a repeating cycle. However, a LFSR with a well-chosen feedback function can produce a sequence of bits which appears random and which has a very long cycle.

1.77. Longer Basis:

See Basis – Longer above.

1.78. Malleability:

If a signature scheme is malleable, we can derive another signature of the message, from any message-signature pair. This is the weakness of the original NTRUSign encryption algorithm in that one can derive many different signatures of the same message.

1.79. Man in the Middle Attack (MITM):

In cryptography, a man-in-the-middle attack (MITM) is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims. The MITM attack is particularly applicable to the original Diffie-Hellman key exchange protocol, when used without authentication. With the exception of the Interlock Protocol, all cryptographic systems that are secure against MITM attacks require an additional exchange or transmission of information over some kind of secure channel. Many key agreement methods with different security requirements for the secure channel have been developed. The MITM attack may include one or more of:

- eavesdropping, including traffic analysis and possibly a known plaintext attack;
- chosen ciphertext attack, depending on what the receiver does with a message that it decrypts;
- substitution attack;
- replay attacks;
- denial of service attack.

1.80. Master Keys:

See Data Keys above.

1.81. Message Authentication Code (MAC):

A cryptographic message authentication code (MAC) is a short piece of information used to authenticate a message. A MAC algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a tag). The MAC value protects both a message's integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

While MAC functions are similar to cryptographic hash functions, they possess different security requirements. To be considered secure, a MAC function must resist existential forgery under chosen-plaintext attacks. This implies that an attacker be unable to find any two messages M and M' which both produce the same MAC under some unknown secret key, even when the attacker has access to an "oracle" which possesses the secret key and generates MACs for messages of the attacker's choosing. Note that this differs from the property of collision resistance required by a cryptographic hash function: a MAC may be considered secure even if the key-holder can efficiently find collisions.

MACs differ from digital signatures, as MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on keys before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures: any user who can verify a MAC is also capable of generating MACs for other messages.

1.82. Microsoft Challenge Handshake Authentication Protocol (MS-CHAP):

The Challenge-Handshake Authentication Protocol (CHAP) authenticates a user to an Internet access provider. RFC 1994: (http://www.ietf.org/rfc/rfc1994.txt) PPP Challenge Handshake Authentication Protocol (CHAP) defines the protocol. CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link, and may happen again at any time afterward. The verification is based on a shared secret (such as the client user's password).

1. After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.

2. The peer responds with a value calculated using a one-way hash function, such as MD5 (see below).

3. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.

4. At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 to 3.

CHAP provides protection against playback attack by the peer through the use of an incrementally changing identifier and of a variable challenge-value.

1.83. Message-Digest Algorithm 4 (MD4):

MD4 is a message digest algorithm implementing a cryptographic hash function for use in message integrity checks. The digest length is 128 bits. The algorithm has influenced later designs, such as the MD5, SHA and RIPEMD algorithms.

1.84. Message-Digest Algorithm 5 (MD5):

MD5 (Message-Digest algorithm 5) is a widely-used cryptographic hash function with a 128-bit hash value. As an Internet standard (RFC 1321) (http://www.faqs.org/rfcs/rfc1321.html), MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. In 1996, a flaw was found with the design of MD5; while it was not a clearly fatal weakness, cryptographers began to recommend using other algorithms, such as SHA-1 (recent claims suggest that SHA-1 has been broken, however) (see SHA-1 below). In 2004, more serious flaws were discovered making further use of the algorithm for security purposes questionable.

1.85. Mutual Authentication:

Mutual authentication or two-way authentication refers to two parties authenticating each other in such a way that both parties are assured of the others' identity.

1.86. Near Field Communications (NFC):

Near Field Communication Technology or NFC jointly developed by Sony and Philips is an approved standard ISO/IEC 18092. Near Field Communication Technology holds the promise of bringing true mobility to consumer electronics in an intuitive and psychologically comfortable way since the devices can hand-shake only when brought literally into touching distance. A NFC Forum is at http://www.nfc-forum.org/home.

1.87. NIST Test for random numbers:

National Institute of Standards and Technology, USA Publication (SP) 800-22 is a Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. The publication and the associated tests are intended for individuals who are responsible for the testing and evaluation of random and pseudorandom number generators. NIST SP 800-22 is available at http://csrc.nist.gov/rng/

The NIST Statistical Test Suite is a package of 16 tests that were developed to test the randomness of (arbitrarily long) binary sequences produced by random or pseudorandom number generators. The tests focus on a variety of different types of non-randomness that could exist in a sequence.

1.88. Non-invasive Attacks:

These attacks are as a result of timing analysis, power analysis, analysis of certain glitches [radio finger printing], and exploitation of data remanence.

1.89. Non-Malleability:

Non-malleability is a crucial property of a signature scheme. See malleability (see above).

1.90. Non-Repudiation:

In regard to digital security, non-repudiation means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively. In other words, non-repudiation of origin proves that data has been sent, and non-repudiation of delivery proves it has been received.

1.91. Norm – Bound:

A bound of parameter for verification. See NTRUSign below.

1.92. Norm – Centred:

Also known as Centred Norm, see Centred Norm above.

1.93. Norm – Euclidean:

Also known as Euclidean Norm, see Euclidean Norm above.

1.94. NTRUEncrypt Lattice:

The Lenstra–Lenstra–Lovász lattice basis reduction (LLL) is a polynomial time algorithm which, given a lattice basis as input, outputs a basis with short, nearly orthogonal vectors. More precisely, given as input d lattice basis vectors with n-dimensional integer coordinates and a norm lesser than B, the LLL algorithm outputs an LLL-reduced lattice basis in time $O(d^5 n \log_3 B)$. The original application was to give a polynomial time algorithm for factorizing polynomials with rational coefficients into irreducible polynomials. The LLL algorithm has found numerous other applications in cryptanalysis of public-key encryption schemes: knapsack cryptosystems, RSA with particular settings, NTRUEncrypt, and so forth. NTRUEncrypt, also known as the NTRU encryption algorithm, is an asymmetric key encryption algorithm for public key cryptography. NTRUEncrypt employs certain rings of polynomials with convolution multiplication. It relies on the presumed difficulty of factoring certain polynomials in such rings into a quotient of two polynomials having very small coefficients. Breaking the cryptosystem is strongly related, though not equivalent, to the algorithmic problem of lattice reduction (solving the closest vector problem) in certain lattices. Careful choice of parameters is necessary to thwart some published attacks. Since both encryption and decryption use only simple polynomial multiplication, these operations are very fast compared to other asymmetric encryption schemes, such as RSA, El Gamal and elliptic curve cryptography.

1.95. NTRUSign:

NTRUSign, also known as the NTRU Signature Algorithm, is a public key cryptography digital signature algorithm based on the GGH signature scheme. NTRUSign involves mapping a message to a random point in 2N-dimensional space, where N is one of the NTRUSign parameters, and solving the close vector problem in a lattice closely related to the NTRUEncrypt lattice. This lattice has the property that a private 2N-dimensional basis for the lattice can be described with 2 vectors, each with N coefficients, and a public basis can be described with a single N-dimensional vector. This enables public keys to be represented in O(N) space, rather than O(N^2) as is the case with other lattice-based signature schemes. Operations take O(N^2) time, as opposed to O(N^3) for elliptic curve cryptography and RSA private key operations. NTRUSign is therefore claimed to be faster than those algorithms at low security levels, and considerably faster at high security levels. NTRUSign is not a zero-knowledge signature scheme and a transcript of signatures leaks information about the private key. The current proposals use perturbations to increase the transcript length required to recover the private key: the effect of this is that the point representing the message is displaced by the signer by a small secret amount before the signature itself is calculated. The contribution of the perturbations to the transcript is designed to be difficult to distinguish from the contribution of the private key. NTRU claim that at least 230 signatures are needed, and probably considerably more, before a transcript of perturbed signatures enables any useful attack. NTRUSign is under consideration for standardization by the IEEE P1363 working group.

1.96. Object Specific Data:

Object Specific Data is a generic term for information which is characteristic for an item, e.g. its weight, colour, dimensions, etc. It, if carefully chosen, may resemble a "fingerprint" of an object.

1.97. One Time Codes (One Time Pad):

A one-time pad, sometimes called the Vernam cipher, uses a string of bits that is generated completely at random. The keystream is the same length as the plaintext message and the random string is combined using bitwise XOR with the plaintext to produce the ciphertext. Since the entire keystream is random, even an opponent with infinite computational resources can only guess the plaintext if he or she sees the ciphertext.

1.98. One Way (Hash) Function:

A hash function, H, is defined, by h = H(m), where m is the message, and h, is the hash value. The requirements for cryptographic hash functions are:

(a) The input may be of any length;

(b) The output must have a fixed size;

(c) Hash function z = H(k) is comparatively easy to calculate, for any given k;

(d) H(m) is one-way, i.e. is hard to invert, infeasible, computationally, to obtain, k = z^{-1}, or H^{-1} (k), where z = H(k);

(e) H(m) is collision free.

1.99. ONS:

The Object Naming Service is a component of the EPCglobal Network that uses the Internet's existing Domain Name System [DNS] for looking up (resolving) information about an EPC. The term DNS is used when the discussion is generally applicable to the DNS system. ONS is used when the discussion is specifically about querying the DNS to resolve an EPC.

1.100. Passive Adversary:

In Security and Authentication context a Passive Adversary is a malicious entity whose knowledge, hacking skills and resources are limited when compared to an Active Adversary who is assumed to have greater knowledge, skills and resources to hack into a secure system or crack a particular security protocol. Most of the security related literature defines different capabilities (skills and resources) for passive and active adversaries in order to test/prove the security of the proposed system/scheme.

1.101. Physical Attack (Physical Detecting Attack):

In RFID systems the labels themselves are exposed to physical attacks due to the absence of tamper proofing as dictated by cost limitations of low cost tags. Physical attacks are possible irrespective of whether measures are in place to protect labels. The majority of physical attacks possible on devices in general can be bundled into two broad categories based on the means used for accessing the device. An adversary who has the technical equipment, to analyse the tag chip, reverse engineer it, and even read memory its contents, to acquire secret data.

1.102. Plaintext:

Plaintext is the original message, prior to encryption, or the message obtained after decryption, both of which should be the same, if the correct encryption/decryption process was used.

1.103. Polynomial:

In mathematics, a polynomial is an expression in which a finite number of constants and variables are combined using only addition, subtraction, multiplication, and positive whole number exponents (raising to a power).

1.104. Polynomial – Binary:

A polynomial (for example $x^2 + x + 1$) whose variable x can only take values in {0,1}.

1.105. Product Authentication:

Auto-ID technologies such as barcodes and RFID tags can be used to uniquely identify physical objects – but there is a need to ‘bind’ that unique ID to specific characteristics of the physical object, to prevent against the use of duplicate / cloned tags – or genuine tags which have been removed from the original objects and attached to counterfeit goods or unauthorized parts.

The legitimate manufacturer of an object may store information in their database against each unique ID about particularly characteristics of each individual object they create, such as its date of manufacture, precise weight, photographs, any mass-customized security markings (covert or overt), which would allow authorized authenticated clients to query to check that the ID they read from the RFID tag or barcode matches the physical object carrying that particular ID. This verification process is known as Product Authentication since the emphasis is on checking that the ID corresponds to a particular physical object.

1.106. Pseudorandom Number Generator:

A pseudorandom number generator (PRNG) is an algorithm that generates a sequence of numbers which are not truly random. The outputs of pseudorandom number generators only approximate some of the properties of random numbers. Although truly random numbers are believed to be generatable using hardware random number generators, pseudo-random numbers are central in the practice and so in the theory of cryptography. Careful mathematical analysis is required to have any confidence a PRNG generates numbers that are sufficiently "random" to suit the intended use.

1.107. Public Key Cryptography Systems:

Public key cryptography is a form of cryptography which generally allows users to communicate securely without having prior access to a shared secret key. This is done by using a pair of cryptographic keys, designated as public key and private key, which are related mathematically. In public key cryptography, the private key is kept secret, while the public key may be widely distributed. In a sense, one key "locks" a lock; while the other is required to unlock it. It should not be possible to deduce the private key of a pair given the public key, and in high quality algorithms no such technique is known. There are many forms of public key cryptography, including:

- public key encryption — keeping a message secret from anyone that does not possess a specific private key;
- public key digital signature — allowing anyone to verify that a message was created with a specific private key;
- key agreement — generally, allowing two parties that may not initially share a secret key to agree on one.

1.108. Public Key Challenge Response:

A public key is an encryption key used in asymmetric encryption, which allows both creation of digital signatures and decryption. A public key is made available to everyone in public key cryptography system and is used in conjunction with a private key. Users can digitally sign messages using private keys, and another party can check that signature using the public key.

1.109. Public Key Infrastructure:

Public key infrastructure (PKI) is an arrangement that provides for trusted third party vetting of, and vouching for, user identities.

1.110. Public/Private Keys:

A key is a constant number which is used in the encryption/decryption process. The public key is used to encrypt messages and can be insecure, but the private key must be confidentially exchanged between the originator (source) and receiver (destination).

1.111. PUF (Physically Unclonable Functions):

In RFID PUF circuits may be exploited to provide a source of truly random bit sequences, to be used in a challenge-response protocol exchange in security and authentication applications. The technique employs a PUF (Physically Unclonable Function) circuit which has an exponential number of delay path configurations determined by a challenge input. The observation of PUF results reveals that a string of challenge bit sequences can be used to generate a response string unique to each IC. The PUF circuit is able to uniquely characterise each IC due to manufacturing variations. These individual characteristics then become similar to the secret keys used in a symmetrical encryption scheme. Thus, it is possible to identify and authenticate each IC reliably by observing the PUF response.

1.112. Quality of Service (QoS):

In the fields of packet-switched networks and computer networking, the traffic engineering term Quality of Service (QoS) refers to the probability of the telecommunication network meeting a given traffic contract, or in many cases is used informally to refer to the probability of a packet succeeding in passing between two points in the network within its desired latency period.

1.113. Quotient Polynomial Ring:

A quotient polynomial ring is the set of polynomials in one or more variables with coefficients in a ring. See Quotient Ring below.

1.114. Quotient Ring:

In mathematics a quotient ring, also known as factor ring or residue class ring is a construction in ring theory, quite similar to the factor groups of group theory and the quotient spaces of linear algebra. One starts with a ring R and a two-sided ideal I in R, and constructs a new ring, the quotient ring R/I, essentially by requiring that all elements of I be zero. Intuitively, the quotient ring R/I is a "simplified version" of R where the elements of I are "ignored".

1.115. Replay Attack:

A replay attack is one in which an attacker monitors transactions (messages) between two communicating parties, record the transactions and use parts of the messages to illicitly obtain information. Retransmission of such recorded information may be used to attack the communication system.

1.116. Reverse Engineering:

Reverse engineering is the process of discovering the technological principles of an application through analysis of its structure, function and operation, usually with the intention to construct a new device or program that does the same thing without actually copying anything from the original.

1.117. RIPEMD (RIPEMD-160):

RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest) is a 160-bit message digest algorithm (and cryptographic hash function). It is an improved version of RIPEMD, which in turn was based upon the design principles used in MD4, and is similar in performance to the more popular SHA-1. There also exist 128, 256 and 320-bit versions of this algorithm, called RIPEMD-128, RIPEMD-256, and RIPEMD-320, respectively. The 128-bit version was intended only as a drop-in replacement for the original RIPEMD, which was also 128-bit, and which had been found to have questionable security. The 256 and 320-bit versions diminish only the chance of accidental collision, and don't have higher levels of security as compared to, respectively, RIPEMD-128 and RIPEMD-160.

1.118. RSA:

In cryptography, RSA is an algorithm for public-key encryption. The algorithm was described in 1977 by Ron Rivest, Adi Shamir and Len Adleman at MIT; the letters RSA are the initials of their surnames. RSA involves two keys: a public key and a private key. The public key is known to everyone and is used to encrypt messages. These messages can only be decrypted by use of the private key. In other words, anybody can encrypt a message, but only the holder of a private key can actually decrypt the message and read it.

1.119. Secure Shell (SSH):

Secure Shell or SSH is a set of standards and an associated network protocol that allows establishing a secure channel between a local and a remote computer. It uses public-key cryptography to authenticate the remote computer and (optionally) to allow the remote computer to authenticate the user. SSH provides confidentiality and integrity of data exchanged between the two computers using encryption and message authentication codes. SSH is typically used to login to a remote machine and execute commands, but it also supports tunnelling, forwarding arbitrary TCP ports and X11 connections; it can transfer files using the associated SFTP or SCP protocols. An SSH server, by default, listens on the standard TCP port 22.

1.120. Secure Hash Algorithm SHA-1:

The SHA (Secure Hash Algorithm) family is a set of related cryptographic hash functions. The most commonly used function in the family, SHA-1, is employed in a large variety of popular security applications and protocols, including TLS, SSL, PGP, SSH, S/MIME, and IPSec. SHA-1 is considered to be the successor to MD5, an earlier, widely-used hash function. The SHA algorithms were designed by the National Security Agency (NSA) and published as a US government standard. The first member of the family, published in 1993, is officially called SHA; however, it is often called SHA-0 to avoid confusion with its successors. Two years later, SHA-1, the first successor to SHA, was published. Four more variants have since been issued with increased output ranges and a slightly different design: SHA-224, SHA-256, SHA-384, and SHA-512 — sometimes collectively referred to as SHA-2.

Attacks have been found for both SHA-0 and SHA-1. No attacks have yet been reported on the SHA-2 variants, but since they are similar to SHA-1, researchers are worried, and are developing candidates for a new, better hashing standard.

1.121. Secure Socket Layer (SSL):

See Transport Layer Security (TLS) below.

1.122. Security Ranks:

As the security methods employed on tag chips increases, the complexity of hardware and the area also increase. Various applications require different security provisions, and in RFID tag applications four levels of security rank are defined:

- Level 1: Supporting the authentication mechanism between each other (Reader and Tag);
- Level 2: Level 1 functionality and cover coding the messages sent by the reader to the tag in the forward channel;
- Level 3: Level 2 functionality as well as cover coding the messages sent by tag to reader in the backward channel, in addition with each transmission using different cryptographic values to avoid trace;
- Level 4: Level 4 functionality and restricting the reader's accessing number (Readers to have unique identities).

1.123. Security Vulnerabilities:

Security vulnerability refers to a weakness in a system allowing an attacker to violate the integrity, confidentiality, access control, availability, consistency or audit mechanism of the system or the data and applications it hosts. Vulnerabilities may result from bugs or design flaws in the system. A vulnerability can exist either only in theory, or could have a known exploit. Vulnerabilities are of significant interest when the program containing the vulnerability operates with special privileges, performs authentication or provides easy access to user data or facilities.

1.124. Seed:

Arbitrary initial state of a pseudorandom number generator.

1.125. Side Channel Attack:

In cryptography, a side channel attack is any attack based on information gained from the physical implementation of a cryptosystem, rather than theoretical weaknesses in the algorithms. For example, timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information which can be exploited to break the system. Many side-channel attacks require considerable technical knowledge of the internal operation of the system on which the cryptography is implemented.

1.126. Short Basis:

See Basis – Short above.

1.127. SQL Injection Vulnerability:

See Code Injection Vulnerability above.

1.128. SSHA-512

The SHA (Secure Hash Algorithm) family is a set of related cryptographic hash functions. The SHA algorithms were designed by the National Security Agency (NSA) and published as a US government standard. SHA-512 is a successor of the original algorithm and specified under FIPS PUB 180-2. http://www.infosec.gov.hk/english/general/glossary.htm

1.129. Stack Smashing Attack:

Stack smashing attacks refers to various techniques used by attackers to compromise the security of a computer system, by causing a buffer overflow, on stack-allocated variables. See Heap Smashing Attack above for another kind of buffer overflow attack.

1.130. Symmetric Key System:

A symmetric key system is a cryptographic system in which both the sender and the receiver use the same keys.

1.131. Tag Cloning:

See Clone above.

1.132. TCP/IP:

The internet protocol suite is the set of communications protocols that implement the protocol stack on which the Internet and most commercial networks run. It is sometimes called the TCP/IP protocol suite, after the two most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which were also the first two defined. TCP/IP is composed of layers:

- IP - is responsible for moving packet of data from node to node. IP forwards each packet based on a four byte destination address (the IP number).
- TCP - is responsible for verifying the correct delivery of data from client to server. Data can be lost in the intermediate network. TCP adds support to detect errors or lost data and to trigger retransmission until the data is correctly and completely received.

1.133. Tracing Attack:

An adversary who uses simple RF transmitters (may be RFID Readers) and RF detectors (also could be an RFID reader) to detect and trace RFID tags after sending some small instructions. This adversary can therefore locate and track the tag and hence the object that the tag is attached to, illegally.

1.134. Transport Layer Security (TLS):

Secure Sockets Layer (SSL) and Transport Layer Security (TLS), its successor, are cryptographic protocols which provide secure communications on the Internet. There are slight differences between SSL 3.0 and TLS 1.0, but the protocol remains substantially the same.

The first definition of TLS appeared in RFC 2246: "The TLS Protocol Version 1.0". The current approved version is 1.1, which is specified in RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1".

Other RFCs subsequently extended TLS, including:

- RFC 2712: "Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)". The 40-bit cipher suites defined in this memo appear only for the purpose of documenting the fact that those cipher suite codes have already been assigned.
- RFC 2817: "Upgrading to TLS Within HTTP/1.1", explains how to use the Upgrade mechanism in HTTP/1.1 to initiate Transport Layer Security (TLS) over an existing TCP connection. This allows unsecured and secured HTTP traffic to share the same well known port (in this case, http: at 80 rather than https: at 443).
- RFC 2818: "HTTP Over TLS", distinguishes secured traffic from insecure traffic by the use of a different 'server port'.
- RFC 3268: "AES Cipher suites for TLS". Adds Advanced Encryption Standard (AES) cipher suites to the previously existing symmetric ciphers.
- RFC 3546: "Transport Layer Security (TLS) Extensions", adds a mechanism for negotiating protocol extensions during session initialisation and defines some extensions.
- RFC 4279: "Pre-Shared Key Cipher suites for Transport Layer Security (TLS)", adds three sets of new cipher suites for the TLS protocol to support authentication based on pre-shared keys.
- RFC 4347: "Datagram Transport Layer Security" specifies a TLS variant that works over datagram protocols (such as UDP).
- RFC 4366: "Transport Layer Security (TLS) Extensions" describes both a set of specific extensions, and a generic extension mechanism.

The SSL protocol exchanges records; each record can be optionally compressed, encrypted and packed with a message authentication code (MAC). Each record has a content_type field that specifies which upper level protocol is being used.

When the connection starts, the record level encapsulates another protocol, the handshake protocol, which has content_type 22.

The client sends and receives several handshake structures:

1. It sends a ClientHello message specifying the list of cipher suites, compression methods and the highest protocol version it supports. It also sends random bytes which will be used later.

2. Then it receives a ServerHello, in which the server chooses the connection parameters from the choices offered by the client earlier.

3. When the connection parameters are known, client and server exchange certificates (depending on the selected public key cipher). These certificates are currently X.509, but there's also a draft specifying the use of OpenPGP based certificates.

4. The server can request a certificate from the client, so that the connection can be mutually authenticated.

5. Client and server negotiate a common secret called "master secret", possibly using the result of a Diffie-Hellman exchange, or simply encrypting a secret with a public key that is decrypted with the peer's private key. All other key data is derived from this "master secret"

(and the client- and server-generated random values), which is passed through a carefully designed "Pseudo Random Function".

1.135. TLS/SSL protocols have a variety of security measures:

1. Numbering all the records and using the sequence number in the MACs.

2. Using a message digest enhanced with a key (so only with the key can you check the MAC). This is specified in RFC 2104).

3. Protection against several known attacks (including man in the middle attacks), like those involving a downgrade of the protocol to previous (less secure) versions, or weaker cipher suites.

4. The message that ends the handshake ("Finished") sends a hash of all the exchanged data seen by both parties.

5. The pseudo random function splits the input data in 2 halves and processes them with different hashing algorithms (MD5 and SHA), then XORs them together. This way it protects itself in the event that one of these algorithms is found vulnerable.

1.136. Trap Door One Way Function:

A trapdoor function is a function that is easy to compute in one direction, yet believed to be difficult to compute in the opposite direction (finding its inverse) without special information, called the "trapdoor". Trapdoor functions are widely used in cryptography. In mathematical terms, if f is a trapdoor function there exists some secret information y, such that given f(x) and y it is easy to compute x. For example if [$y=x^n$]mod(p), mod(p) is the secret information, and p is usually a prime number. Without the mod(p) it may be easy for an eavesdropper to map the values transmitted and guess that the sequence fits an exponential curve and hence calculate x.

1.137. Trojan Attack or Trojan Horse:

A Trojan horse is a malicious program that is disguised as or embedded within legitimate software. They may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed. There are two common types of Trojan horses. One, is otherwise useful software that has been corrupted by a cracker inserting malicious code that executes while the program is used. Examples include various implementations of weather alerting programs, computer clock setting software, and peer to peer file sharing utilities. The other type is a standalone program that masquerades as something else, like a game or image file, in order to trick the user into some misdirected complicity that is needed to carry out the program's objectives. Trojan horse programs cannot operate autonomously, in contrast to some other types of malware, like viruses or worms. Trojan horse programs depend on actions by the intended victims. As such, if trojans replicate and even distribute themselves, each new victim must run the program/trojan.

1.138. Unauthenticated Access Attack:

An adversary, who uses a real RFID reader to gain unauthenticated access to RFID tags, in order to collect secret information.

1.139. Untraceability:

Untraceability is the property that an adversary cannot trace the RFID Tag (T) by using interactions with T.

1.140. User Datagram Protocol (UDP):

The User Datagram Protocol (UDP) is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages known as datagrams to one another. UDP can also stand for "Unreliable". It doesn't mean you will lose all your data, but it does not provide the reliability and ordering guarantees that TCP does. Datagrams may arrive out of order or go missing without notice. Without the overhead of checking if every packet actually arrived, UDP is faster and more efficient for many lightweight or time-sensitive purposes. Also its stateless nature is useful for servers that answer small queries from huge numbers of clients. Compared to TCP, UDP is required for broadcast (send to all on local network) and multicast (send to all subscribers). Common network applications that use UDP include the Domain Name System (DNS), streaming media applications, Voice over IP, Trivial File Transfer Protocol (TFTP), and online games.

1.141. Verification:

Verification is the process of checking the truth with an authoritative source. Verification of digital signatures consists of decryption of the digital signature using the signer’s public key and comparison of the result with the message digest or hash value which is obtained by processing the signed data content using the hashing algorithm specified in the digital certificate. The link between the public key and its owner should also be verified – usually involving a network lookup via a certificate authority. Certificate authorities are used to provide chains of trust to act as an authority about who owns a particular public key.

1.142. Virtual Private Network (VPN):

A virtual private network (VPN) is a private communications network usually used within a company, or by several different companies or organizations, to communicate over a public network. VPN message traffic is carried on public networking infrastructure (e.g. the Internet) using standard (often insecure) protocols, or over a service provider's network providing VPN service guarded by well-defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider.

VPN involves two parts:

(1) The protected or "inside" network that provides physical security and administrative security sufficing to protect transmission, and

(2) A less trustworthy or "outside" network or segment (the internet).

Generally, a firewall sits between a remote user's workstation or client and the host network or server. As the user's client establishes the communication with the firewall, the client may pass authentication data to an authentication service inside the perimeter. Many VPN client programs can be configured to require that all IP traffic must pass through the tunnel while the VPN is active, for better security. From the user's perspective, this means that while the VPN client is active, all access outside their employer's secure network must pass through the same firewall as would be the case while physically connected to the office ethernet.

1.143. Whirlpool:

WHIRLPOOL is a cryptographic hash function adopted by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as part of the joint ISO/IEC 10118-3 international standard. WHIRLPOOL is a hash designed after the Square block cipher. WHIRLPOOL is based on a substantially modified Advanced Encryption Standard (AES). Given a message less than 2256 bits in length, it returns a 512-bit message digest.

1.144. X.509:

In cryptography, X.509 is an ITU-T standard for public key infrastructure (PKI). X.509 specifies, amongst other things, standard formats for public key certificates and a certification path validation algorithm. In the X.509 system, a Certification Authority (CA) issues a certificate binding a public key to a particular Distinguished Name in the X.500 tradition, or to an Alternative Name such as an e-mail address or a DNS-entry. An organisation's trusted root certificates can be distributed to all employees so that they can use the company PKI system. Browsers such as Internet Explorer, Netscape/Mozilla and Opera come with root certificates pre-installed, so SSL certificates from larger vendors who have paid for the privilege of being pre-installed will work instantly; in essence the browser's owners determine which CAs are trusted third parties. X.509 also includes standards for certificate revocation list (CRL) implementations. The IETF-approved way of checking a certificate's validity is the Online Certificate Status Protocol (OCSP).

Appendix A - Other online sources of terms and glossaries:

http://www.opengroup.org/onlinepubs/008329799/glossary.htm#tagcjh_12

http://www.discretix.com/glossary.shtml

http://www.orionsec.com/Security_Glossary.html

http://www.17799central.com/glossary.htm

http://www.watchguard.com/glossary/?nav=ic

http://www.primode.com/glossary.html

http://www-306.ibm.com/software/webservers/httpservers/doc/v1326/manual/ibm/9agloss.htm

http://www.clusit.it/whitepapers/glossary.htm

http://www.aamc.org/members/gir/gasp/definitions.pdf

http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_GlossaryofTerms.pdf

http://www.infosec.gov.hk/english/general/glossary.htm