CRYPTOGRAPHIC ALGORITHM METRICS

Norman D. Jorstad
Director, Technology Identification and Analyses Center

Landgrave T. Smith, Jr.
landgrave@aol.com

January 1997

Institute for Defense Analyses
Science and Technology Division

20NCDROM
7 Jun 97
BU11

CRYPTOGRAPHIC ALGORITHM METRICS

ACKNOWLEDGMENTS

This paper is the work of a team composed of: Lt. Gen. Lincoln D. Faurer, USAF (Retired), Mrs. Janice L. Freeman, Father M. Blake Greenlee, Mr. D. Richard Kuhn and Mr. Charles W. Shadel. It is essentially a brief status report on a study in progress.

I. PURPOSE

In the absence of generally accepted metrics in the public domain that could be used to measure and specify cryptographic strength, a small working group agreed to explore the possibility of developing an approach to cryptographic metrics

The purpose of this white paper is to report the results of the limited exploratory effort by the above group that investigated the practicality of developing metrics for use in specifying the strength of cryptographic algorithms. This paper only deals with a small sample of selected symmetric cipher block encryption algorithms in the codebook mode and an asymmetric public key algorithm. Other algorithms and cryptographic techniques for message integrity, authentication, and digital signatures were not investigated. Only information available in the public domain was used during this investigation.

Appendix A contains a glossary of acronyms and definitions.

II. BACKGROUND

A. REQUIREMENT

There seems to be an emerging requirement to specify cryptographic strength objectively rather than subjectively with adjectival descriptors such as weak, good or strong. It is expected that U.S. Government (USG) and industry will soon require specific quantitative data to define the point at which a cryptographic technology or product will satisfy user requirements.

This pilot effort on cryptography metrics was originally undertaken to investigate the feasibility of developing only objective, numeric scales with which to specify the characteristics of cryptographic algorithms functioning in the codebook mode. In this limited pilot, an objective metric for algorithm strength was not identified; however, a subjective, adjectival scale is suggested for rating the overall strength of an algorithm.

If such metrics can be developed for describing the attributes of cryptographic products and technologies, they might have future utility for Common Criteria Level of Assurance (LA) statements or evaluations. This cryptographic metrics pilot provides, for the first time, an indication that a framework might be developed for specifying an appropriate set of measures for the strength of cryptographic technologies and products that can be made generally available.

III. APPROACH

A. LOGIC

Although some important characteristics might not be quantifiable, it seems intuitively logical that it should be possible to identify some cryptographic algorithm characteristics that can be expressed either in objective, numeric values or subjective, adjectival values. Metrics might be used for evaluating and comparing cryptographic algorithms and the inferred confidentiality protection value of products containing cryptographic algorithms.

Encryption algorithm characteristics that were considered for the development of metrics:

1. **Type** - *symmetric* (secret key or one-key) or *asymmetric* (public key or two-key). While strictly speaking this may not be a metric, the type of key that an algorithm uses would be of sufficient interest to users to be worth specifying. (Because there are short-cut attacks that can be used on asymmetric algorithms, very long keys are required. With any meaningful key length, two-key algorithms are very slow when compared to one-key algorithms. This effectively limits their use to the management of keys for symmetric algorithms. It should be noted that some two-key algorithms can provide a covert channel for traffic while masquerading as signatures.)

2. **Functions**. Message *secrecy*, message *integrity*, *authentication*, *digital signatures*, like the type of algorithm, may not be a metric *per se* but may be of interest to end users. Export criteria varies with the functionality, among other things.

3. **Key size**. The *Key Length Metric* proposed in this white paper is intended to provide this comparative value.

4. **Rounds**. *Rounds* were considered but may not be an important metric because rounds, like word and block size, are not universal characteristics and may not have great value in specifying meaningful thresholds.

5. **Complexity**. (Algorithm *complexity* for encryption, decryption, and key setup.) These attributes for encryption, decryption and key setup probably could be specified as the number of operations such as bit operations, modular multiplications and modular exponentiations. The number of operations wouldn't change, only the speed of implementation. (This could be complicated if the algorithm can be parallelized.)

6. **Attack**. Best known methods of attack such as *brute force*, *factoring*, *linear* and *differential cryptanalysis* (qualified with whether known or chosen plaintext is provided,) number of *steps* and *time* required for a successful attack.

7. **Strength**. An *assessment* of the strength of the algorithm, based on key length, algorithm complexity and the best methods of attack. A subjective, adjectival cryptographic *Algorithm Strength* metrics scale is proposed in this white paper.

B. SCOPE

This pilot effort was limited to a small set of *civilian* cryptographic algorithms in the public domain used to provide business and personal data confidentiality and integrity in *commercial* cryptographic products. To further limit the effort, only the Electronic Codebook (ECB)[1] mode of operation was investigated since the metric values for each algorithm could vary significantly with the mode of operation. In addition, each mode considered would have multiplied the pilot effort. Since a larger set of modes would have broadened this proof-of-concept pilot unnecessarily, message integrity, authentication and digital signature modes were not investigated.

C. PILOT CHOICE JUSTIFICATION

Civilian business and personal cryptographic system symmetric cipher block algorithms, in the codebook mode for confidentiality protection and an asymmetric public key algorithm, were chosen because they appeared to be the most tractable candidates.

IV. CRYPTOGRAPHIC ALGORITHM METRICS

A. THE FUNCTION OF CRYPTOGRAPHY

Cryptology is the branch of mathematics encompassing both cryptography and cryptanalysis. Modern cryptologists are generally trained in theoretical mathematics and computer science. The art and science of keeping messages secure is *cryptography*, and it is practiced by *cryptographers*. *Cryptanalysts* are practitioners of *cryptanalysis*, the art and science of breaking ciphertext; that is, seeing plaintext through the cryptographic disguise. Cryptology presents a difficulty not found in normal academic disciplines: the need for continuous interaction of cryptography and cryptanalysis. This interaction begins with a challenge from cryptographers that starts each cycle with an announcement of a new algorithm design and a response from the cryptanalysts who try to expose flaws in the design, which is usually far harder than designing the algorithms in the first place. The result is a healthy competitive process that produces "strong" cryptography.

The function of cryptography is transforming (*encrypting*) information with secret keys for the purpose of secrecy or authenticity. A cryptographic system ("*cryptosystem*") or subsystem consists of privacy transformations, authenticity transformations or a combination thereof. Keys parameterize the transformations. Privacy transformations are used to *encrypt* and *decrypt*.[2] The encrypt function transforms intelligible data (called *plaintext* or *cleartext*) into what appears to be

[1] The Electronic Codebook (ECB) mode is a basic, block, cryptographic method, which transforms 64 bits of input to 64 bits of output, as specified in FIPS PUB 46-2. See Appendix B of FIPS Pub 81, *DES Modes of Operation*.

[2] The International Standards Organization (ISO 7498-2) uses the terms "encipher" and "decipher."

unintelligible data (*ciphertext*). The decrypt function transforms ciphertext back to its original form (plaintext). Cryptographic algorithms, which are the mathematical functions used for encryption and decryption that characterize each system, were chosen for this pilot because they appeared to be a tractable subset of the cryptography technologies. Table 1 shows the functionality of some typical algorithms.

Type of Transformation	Typical Algorithms	Functions	Limitations/Other Factors
Privacy	**DES** **3DES** **SKIPJACK** **RC4** **RC5** **RSA** **El Gamal**	**Encrypt** **Decrypt**	**Primary use of RSA and El Gamal (encryption) is key management.**
Authenticity	**DES** **DSA & SHA** **RSA & hash** **El Gamal & hash**	**Compute and verify MAC (DES)** **Sign and verify (DSA & SHA, RSA & hash, El Gamal & hash)**	

Table 1. Examples of Cryptographic Transformations

The functions of encryption algorithms are to provide message secrecy or confidentiality, and message integrity protection (authentication.) Note that the RSA algorithm may be used to *encrypt* or *decrypt*, or to *sign* and *verify*. The Digital Signature Algorithm (DSA), Secure Hash Algorithm (SHA) and El Gamal signature algorithms provide integrity protection through functions that *sign* and *verify*. The examples in Table 1 illustrate these principles. Transformations may be combined.

B. PILOT LIMITATIONS AND PROBLEMS

1. Sample

Only a small (five) sample of algorithms were investigated, some only partially. The cryptographic algorithm dimensions for only the codebook mode of operation were collected for the symmetric cipher block algorithms for this proof-of-concept effort. The Electronic Codebook (ECB) mode is a basic, block, cryptographic method which transforms 64 bits of input to 64 bits of output as specified in FIPS PUB 46-2. Most popular symmetric block cipher algorithms can be used in different modes. The, Data Encryption Standard (DES), a.k.a. Data Encryption Algorithm (DEA), can be used in the Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher

Feedback (CFB) and Output Feedback (OFB) modes, for example. Treating all current modes of each of the symmetric block cipher algorithms in this pilot would have multiplied the effort beyond the likely benefit of any findings and required access to data not readily available.

There were five postulated metrics included in this investigation. Originally, six algorithms were selected as candidate cryptographic algorithms for which data was to be collected (in the confidentiality protection or codebook mode of operation.) Since RC4 data was proprietary, it was eliminated The resulting matrix that appears at the end of the Application Section is believed to be an adequate indication that the development of cryptographic algorithm metrics may be feasible, though a nontrivial task. Perhaps metrics for other information security technology and products are also practicable.

2. Exposure

The value of this pilot also suffers from too narrow an exposure to comment and criticism. The circulation has been limited to the Information Security Technology Working Group metrics team and only two other audiences; the first public presentation at the 1996 RSA Data Security Conference, and the second, at an Information Systems Technical Advisory Committee meeting. Also, the data suffers from incompleteness. Except for the DES algorithm, complete data was not readily available to the authors. Additional resources and the full cooperation of publishers and algorithm developers will be required for further algorithm metrics investigation. If this pilot were published in open literature, it should benefit from a broader base of criticism and additional data may be proffered.

3. Technical Literature Search

Only a limited key-word search of the technical literature published in 1994 and 1995 was made. One interesting article was found, reporting an investigation of CRYPT-X. CRYPT-X is an Australian computer software package used for assessing the security of newly-developed encryption algorithms, which performs eight statistical tests on both stream and block ciphers. The design of these eight tests might provide the bases for better or additional scales.[3]

C. CRYPTOGRAPHIC ALGORITHM METRIC DESCRIPTIONS

1. Key Length Metric

The security of a symmetric cryptosystem is a function of the length of the key. The longer the key, the more resistant the algorithm is to a successful brute force attack. For this reason, key length was chosen as the first parameter for specifying cryptographic algorithms. Key Length is an easy objective, numeric metric to adopt since key size is universally expressed as a number of bits. For example, the standard key length for the Data Encryption Standard (DES) is

[3] H. Gustafson, et al., "A Computer Package for Measuring the Strength of Encryption Algorithms," *Computers & Security*, Vol 13, No. 8, 1994, Elsiver Science, Ltd., pp. 687-697.

56 bits. Assuming there is no better way to break the cryptosystem, other than to try every possible key with a brute force attack, the longer the key, the longer it will take to make the number of attempts necessary to find the correct key. In fact, every extra key bit generally doubles the number of possible keys and therefore increases the effort required for a successful brute force attack against most symmetric algorithms. A key length of *N* bits has 2^N possibilities. Adding an extra key bit does not always exactly double the effort required to break public key algorithms because some public key algorithms may have short-cut attacks such as factoring and computing the discrete log.

2. Attack Steps Metric

Attack Steps is defined as the number of steps required to perform the best known attack. The number of steps helps determine the time that might be required for a successful attack, using a particular processor, without having to actually run the attack on the algorithm, which may not be feasible.

3. Attack Time Metric

Attack Time is defined as the time required to perform the fastest known attack on a specified processor.

a. Computer and Encryption Algorithm Theoretical Operation Assumptions

Composite theoretical performance (CTP) is a measure of computational performance given in *millions of theoretical operations per second* (Mtops), calculated using the aggregation of computing elements. See Appendix B for the COCOM successor regime (Wassenaar Agreement[4]) international procedure for computing *composite theoretical performance* (CTP) in *millions of theoretical operations per second* (Mtops.) For simplification, it was assumed that encryption algorithms evaluated or specified with this metric would use only computational primitive operations commonly found on typical processors and that primitives would be executed in operations of equal times. A cryptanalytic algorithm operation was assumed to have a one to one ratio with (or be equal to) one *theoretical operation* of the processor.

b. Time Granularity

The year time granularity seemed consistent with the precision of the theoretical operation assumptions. A 365 day year was arbitrarily adopted for simplification. A *Mtops year* was defined as a CTP given in Mtops for the arbitrarily selected computer.[5] For example, a machine that operates at 1216 (Mtops) times 60 (seconds/minute) times 60 (minutes/hour) times 24 (hours/day) 365 (days/year) equals 3.83478×10^{10} million operations/year (an Mtops year using the 1216 Mtops machine.) The Mtops year was rounded to two decimal places for Table 3.

[4] The agreement takes it name from the city in The Netherlands where the agreement was formally promulgated.
[5] DEC AlphaServer 2100 4/275, which is rated by the manufacturer at 1216 Mtops.

c. Attack Time Metric Computer Selection

A computer assumed to soon be reasonably available internationally was selected. Computers with a CTP below 500 Mtops have been decontrolled nationally and internationally. In the near future, up to 2000 Mtops computers [the postulated super computer threshold] are expected to be decontrolled by the Wassenaar Agreement countries and the U.S. In fact, processors below 2000 Mtops are already widely available, nationally and internationally, and affordable to those with serious cryptanalytic intentions.[6] Since Attack Time is a function of the processor used, a DEC processor was arbitrarily specified for the computation of the Attack Time estimates that appear in this white paper. The 1216 Mtops (243,200 million instructions per second (MIP)) DEC symmetrical multiprocessor, which is comfortably below 2000 Mtops super computer threshold, was the model selected for computing Attack Times. Of course, changes in information technology must be considered in assessing the longevity of any evaluation of the strength of an encryption algorithm based on attack time. For example, today a pair of these relatively inexpensive symmetrical multiprocessors can perform 2,432 million theoretical operations per second (Mtops) and *each* may have a work space of up to 2 GBytes (gigabyte - a gigabyte is a thousand megabytes, a megabyte is a million bytes) of RAM (random access memory.) It seems reasonable to assume, at least in the near future, that the power of processors will continue to double about every 18 months. Also, the cost of processing power is expected to continue to be halved about every 18 months, making greater processing power less expensive.

4. Rounds Metric

Rounds by themselves may not have great value in specifying meaningful thresholds. (A one-time pad effectively has 1 round and a block size of 1 bit.) However, rounds are important to the strength of some ciphers. For example, an eight-round version of an algorithm like DES is not secure. In general, more rounds lead to greater "confusion" and "diffusion" (Shannon's[7] terminology) and hence more security, up to a point. Because rounds may be representative of a family of easy-to-measure dimensions or characteristics that could indicate speed, the rounds metric was included in the pilot for illustration.

5. Algorithm Strength Metric

This subjective, adjectival metric is meaningful **only** if an objective, numeric key length also is specified. Computation of comparable key lengths for the algorithms chosen for each

---

[6] The new DEC symmetrical multiprocessor, AlphaServer 1000 4/200, rated at 245.7 Mtops, Max SPEC_int92 of 135.8 (135.8 x 200 MIPs, or 27,160 MIPs), $18K; the AlphaServer 2100 4/275 comes in at 1216 Mtops or 243,200 MIPs for $75K. Workstation aggregations linked together to form low latency parallel virtual machines and fiber-distributed data interface (FDDI) interconnected "PC farms" could multiply processor capabilities, reducing attack times significantly.

[7] Shannon, C.E., "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, Vol 28, pp. 656-715, October 1949.

Algorithm Strength scale graduation was beyond the resources of this pilot. Accordingly, comparable key lengths for each graduation remain to be determined.

The security of a cryptosystem should rest on the structure of the algorithm and this security is enhanced if the algorithm is held secret. However, the strength (security) of a cryptosystem must not depend on the secrecy of the algorithm. But, by keeping the algorithm secret, an adversary is forced to expend valuable resources in determining a method of attack. An experienced cryptanalyst, who is also an expert programmer, can disassemble the source code or reverse-engineer the algorithm in software applications. State-of-the-art chip coating and encapsulation fabrication techniques may substantially extend the life of a secret algorithm in hardware applications. But, resourceful engineers might ultimately reverse-engineer the hardware.

Knowing the algorithm should not allow the ciphertext to be broken. Knowledge of the algorithm should not reduce the strength of the cipher, but will substantially reduce the resources required to break the cyptosystem. The DES algorithm has been in the public domain for many years. In this case, the security of DES depends on the complexity of the algorithm and the use of a secret key. Finally, a known plaintext attack against a key should never be allowed. Success can be identified by simple pattern-matching if the plain text is known; otherwise, an attack is much more difficult, but still possible.[8] All American National Standards Institute (ANSI) Accredited Standards Committee, X9 (Financial Services) standards developed since 1982 deny a known plaintext attack on a cipher.

Algorithm strength was chosen as the name of a scale developed for expressing the overall measurement of a cryptographic algorithm's strength, worth or value, even though the scale has to be defined and expressed in subjective, adjectival terms. This is the only subjective, adjectival characteristic scale for algorithm specification that was developed during this pilot. The Algorithm Strength (AS) metric is intended for use by experienced cryptographers to specify, or express an evaluation of, algorithm strength values.

While theoretically breakable, many algorithms are *Computationally Strong* (CS), or practically unbreakable, in the sense that the resources required for timely cryptanalysis are either unavailable or prohibitively expensive. In practice, a system need only be strong enough to provide a level of security commensurate with the risk and consequences of breakage in some specified period of time. Increasing the strength of the cryptographic system usually increases its cost and degrades system performance, so no more resources than the expected resource loss resulting from breakage should be invested in encryption.

A determination of algorithm strength must take into consideration the best known methods of attack and the length of time required to carry out those attacks using current technology. A cipher designated CS could be demoted at any time by the discovery of a new method of attack or an advance in computational technology. For example quantum computers (QC's), with their potential for rapidly factoring the large numbers used in asymmetric public key

[8] Towbridge, Dave, "Public-key Crypto Gives Privacy Power To The People," *Computer Technology Review*, Vol XV, No. 4, April 1995, p 10.

ciphers, might be able to perform in a few seconds the calculations that today would take billions of years on the most powerful classical computers.[9]

a. Suggested Algorithm Strength Evaluation Criteria

A suggested check list of attributes for use by experienced cryptographers seemed appropriate. In using their subjective judgment to assign Algorithm Strength values, consideration of some set of accepted criteria is recommended such as the following:

(1) The plaintext cannot be derived from the ciphertext without use of the key.

(2) There should be no plaintext attack that is better than a brute force attack.

(3) Knowledge of the algorithm should not reduce the strength of the cipher.

(4) There should be no correlation between any input bits or key bits and the output bits. The algorithm should satisfy the *strict plaintext avalanche criterion* (SPAC) and the *strict key avalanche criterion* (SKAC.) For a fixed key to satisfy the SPAC, each bit of the ciphertext block should change with the probability of one half whenever any bit of the plaintext block is complemented. For key changes, the algorithm satisfies the SKAC if, for a fixed plaintext block, each bit of the ciphertext block changes with a probability of one half when any bit of the key changes.

(5) The algorithm should contain a noncommutative combination of substitution and permutation, except for public key algorithms. (Public key algorithms are an exception to this combination criterion since they don't really have permutations. In public key algorithms, there is a single (one round) substitution over the entire block.)

(6) The algorithm should include substitutions and permutations under the control of both the input data and the key. (Not generally true of public key algorithms, as in (5) above.)

(7) Redundant bit groups in the plaintext should be totally obscured in the ciphertext. (This criterion applies to block ciphers only, which do this within a block.)

(8) The length of the ciphertext should be the same length as the plaintext.

(9) Any possible key should produce a strong cipher, although this is not always true for many good algorithms such as DES and most public key algorithms.

b. Suggested Algorithm Strength Scale Graduations

[9] Glanz, James, "A Quantum Leap for Computers?," *Science*, Vol. 269, 7 July 1995, pps 28 - 29.

Subjective strength definitions for a proposed five graduation Algorithm Strength scale are outlined below.

Graduations	**Definitions**
US	A cipher is **U**nconditionally **S**ecure if, no matter how much ciphertext is intercepted, there is not enough information in the ciphertext to determine the plaintext uniquely.[10] (This definition excludes algorithms which are subject to a plaintext-ciphertext attack and algorithms which permit the attacker to reduce the possible plaintext message to one of two values.)
CS	A cipher is **C**omputationally **S**ecure, or strong, if it cannot be broken by systematic analysis with available resources in a short enough time to permit exploitation.
CCS	A cipher is **C**onditionally **C**omputationally **S**ecure, if the cipher could be implemented with keys that are not quite "long enough" or with not quite "enough" rounds to warrant a CS rating.
W	A **W**eak cipher is one that can be broken by a brute force attack; i.e., the key can be recovered in an acceptable length of time (24 hours) with an "affordable" investment ($200K) in cryptanalytic resources by searching every possible key. A cipher also would be weak if its structure permitted a short-cut method of attack such as differential cryptanalysis.
VW	A **V**ery **W**eak cipher is one that can be broken by determining the key systematically in a short period of time (8 hours) with a small investment ($20K) in cryptanalysis resources.

V. APPLICATION

To provide a small representative sampling of well known cryptographic algorithms, six were originally selected: five symmetric or secret key (one-key) block ciphers and one asymmetric or public key (two-key) algorithm.

1. DES (DEA)

The Data Encryption Standard (DES), a.k.a. the Data Encryption Algorithm (DEA), was the first symmetric block cipher chosen because the DES is a long standing federal standard[11] and

[10] Denning, Dorothy E., *Cryptography and Data Security*, Addison-Wesley Publishing Company, Reading, Massachusetts, January 1983, p.3.
[11] Currently FIPS PUB 46-2, 30 December 1993.

the DEA has been adopted by the American National Standard Institute (ANSI) as a standard[12] and is incorporated in several international standards. DES has been extensively studied since it was first issued as a standard in 1977 and found to be mathematically sound. As required by the standard, DES has been reviewed every five years and was reaffirmed in 1983 and 1988. The third review was conducted in 1993 and DES has been reaffirmed (for the third time) until 1998 as Federal Information Processing Standard Publication (FIPS PUB) 46-2. The National Institute of Standards and Technology (NIST) believes that DES provides adequate security for its intended *unclassified information*[13] applications. The DES algorithm can be used in any one of the four operating modes[14] defined in FIPS 81. The parameters chosen for illustration in this pilot are for DES when used in the Electronic Codebook (ECB) mode.

The algorithm specified in the DES is very complex. It encrypts data in 64 bit blocks, using a 56-bit secret key. There are 2^{56} or about 7.2×10^{16} possible keys[15] for DES. There are four "weak" keys that, if selected, may decrease the security of DES by a factor of two. (When keys are randomly generated, an adversary never knows if a "weak" key is used, hence no keys are weak for a well designed system.) The best attacks on DES that are known are the brute force attack and differential and linear cryptanalyses. (Differential and linear cryptanalyses both are computationally complex.)

Successful cryptanalytic attacks, in general, require substantial quantities of plaintext-ciphertext pairs. It is clear that a single, known plaintext attack against DES (ECB mode) ultimately can be successfully mounted using large massively parallel processing machines available today, given no time constraints. Such an attack should not be successful against DES if the system denies an adversary access to plaintext-ciphertext pairs.

The DES algorithm and key length have been controversial issues ever since the DES was made public. The debate continues on whether or not DES keys can be discovered by today's supercomputers with a brute force computational attack, trying all possible keys, at a cost and in a length of time that would have any practical utility. DES has been one of the most successful and widely used secret key cryptographic systems. Major banking firms around the world rely on this algorithm to protect electronic fund transfers. Some have depended on DES for more than fifteen years.

2. 3DES (EDE)

Triple DES (3DES), a.k.a. Encrypt-Decrypt-Encrypt[16] (EDE) and the Triple Data Encryption Algorithm (TDEA)[17], is the name now most often given one popular form of multiple DES applications. Most 3DES implementations use two keys; however, 3DES can use two or three

---

[12] American National Standard X3.92-1981/R1987.

[13] The term unclassified information excludes classified information covered by 10 USC. 2315.

[14] The modes included in this standard are the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode.

[15] To be exact, 72,057,594,037,927,936 possibilities.

[16] The name a few years ago, when IBM originally suggested this particular multi-pass usage of DES. See Schneier, *E-Mail Security*, John Wiley & Sons, NY, 1995, p. 343.

[17] ANSI nomenclature.

keys. Since DES is (mathematically) not a group[18], the resultant 3DES (using two keys) ciphertext is much harder to break using the exhaustive search method; 2^{112}, instead of 2^{56} attempts are required.[19] There is not complete agreement among authorities that the effective key length of 3DES is really 112. To meet the requirements of the financial community for stronger cryptography, while preserving their investment in DES, ANSI Working Group X9.F.1 is developing American National Standard X9.52 - 19XX, *Triple Data Encryption Algorithm and Modes of Operation*. The X9.52 ANSI standard is expected to include modes that will allow two or three different keys, which would produce an effective key length of 112 or 168 bits, respectively. It should be noted that multiple DES implementations (like the ANSI "Triple Data Encryption Algorithm (TDEA)") provide minimal additional security against a differential cryptanalytic attack[20] as indicated in Table 2:

Number of DES Encryptions	Advantages over Single DES Against a Differential Cryptanalytic Attack
1	**1 (none)**
2	**factor of 2**
3	**factor of 4**
n	**factor of $2^{(n-1)}$**

Table 2. Multiple DES Implementation Advantages

A 56 bit key and 2^{56} trials for a brute force attack were used for the Table 3 illustration in paragraph 7 below, although Mitsuru Matsui[21] has claimed that he experimentally succeeded in breaking the DES with an improved version of linear cryptanalysis in 2^{43} steps.

3. SKIPJACK

SKIPJACK was chosen because it is required by the Escrow Encryption Standard (EES), which is published by National Institute of Standards and Technology (NIST) as a Federal Information Processing Standard publication (FIPS PUB 185.) SKIPJACK is the name given a classified algorithm that operates on 64-bit blocks. The transformation is parameterized by an 80-bit key, and involves performing 32 steps or iterations of a complex, nonlinear function. Like DES, the algorithm can be used in any one of the four operating modes defined in FIPS 81. The parameters chosen for illustration in this pilot are for SKIPJACK when used in the Electronic Codebook (ECB) mode. An independent evaluation team made up of experts outside the U.S. government concluded that it will be 36 years before the cost of breaking SKIPJACK by

[18] K. W. Campbell and M.J. Wiener, "Proof that DES is Not a Group," *Advances in Cryptology - CRYPTO '92 Proceedings*, Berlin; Springer-Verlag, 1993, pp. 518-526. (If DES were a group, cryptanalysis would be easier.)

[19] Triple DES with two keys has attacks requiring less than exhaustion on a full 112-bit key. See paper by Burt Kalisky.

[20] The data presented in Table 2 was derived by Father Blake Greenlee using the equations contained in Don Coppersmith's paper, *A Chosen-Ciphertext Attack on Triple DES CBC*, IBM Research Division, T.J. Watson Research Center, Yorktown Heights, NY 10598, 13 January 95.

[21] Matsui, Mitsuru, "*Linear Cryptanalysis of DES Cipher (I).*" Version 1.03, Computer & Information Systems Laboratory, Mitsubishi Electric Corporation, March 1994.

exhaustive search will be equal to the cost of breaking DES today and that there is no significant risk of SKIPJACK being broken through a shortcut method of attack.[22]

4. RC4™

Dr. Ronald L. Rivest's RC (Ron's Code) 4 was initially chosen as a candidate because it is an established commercial single-key algorithm that accepts a variable key length. Unfortunately, RSA Data Security, Inc., apparently still regards this algorithm as a "trade secret." Access to proprietary documents that contain the complete specification for RC4 would presumably require a nondisclosure agreement. Since one of the ground rules for this pilot was that only information in the public domain would be used, RC4 was dropped after Version 3 of this white paper.

5. RC5™

RC5 was chosen because it is a new fast, symmetric block cipher and the dimensions for the metrics proposed in this pilot were readily available in Dr. Rivest's article in the January 1995 issue of *Dr. Dobb's Journal*. The RC5 is suitable for both hardware or software implementations. A novel feature of RC5 is the heavy use of data-dependent rotations. RC5 has a variable-length secret key, providing flexibility in its security level. It is a parameterized algorithm, and a particular RC5 algorithm is designated RC5-w/r/b, where w is the word size in bits, r is the number of rounds, and b is the number of bits in the secret key. The 64 bit key length used in Table 3 below was chosen arbitrarily for illustration. RC5 provides for the use of up to a 255 bit key.[23]

Since RC5 uses variable length keys and number of rounds, statements that are made about its strength must be made in relation to specified key lengths and rounds; and, Algorithm Strength ratings must be qualified with a specification of these variables. During this pilot, there was not enough time to determine the comparable key lengths that would be required for similar levels of strength for the algorithms investigated.

6. RSA™

The Rivest-Shamir-Adleman (RSA) asymmetric public key cipher is named for its creators: R.L. Rivest, A. Shamir and L.M. Adleman, who were all members of the Massachusetts Institute of Technology (MIT) Laboratory for Computer Science when they developed the public key implementation of the Diffie-Hellman concept. RSA was chosen because it is popular and has been extensively analyzed. RSA is a widely advertised commercial public key algorithm used in business and personal communications. The RSA variable key size may be anywhere from 2 to 2,048 bits in current implementations. The security of these algorithms depends on the key size that the user or programmer chooses.[24] A key length of 1024 bits was used for the illustration in the table below even though many applications are still being fielded with a 512 bit key. (Dr.

---

[22] Brickell, Earnest F., et al, SKIPJACK Review Interim Report, *The SKIPJACK Algorithm*, Sandia National Laboratories, 28 July 1993, p. 1.

[23] With "enough" rounds and a 255 bit key, an RC5 brute force attack would require 2.61×10^{92} years using the DEC AlphaServer™ 2100 4/275.

[24] The RSA key is usually at least 512.

Rivest does not recommend the 512 bit key for any current application. He now recommends a 768 minimum for RSA, and encourages the use of 1024 bits or more. Dr. Rivest believes that the use of a 512 bit key is unwise except for very short-term, very low-security applications.[25])

7. Metrics Application Illustration

Table 3 shows the selected algorithms and illustrates their characteristics as they might be measured and specified with the proposed metrics. The Algorithm Strength scale obviously needs finer granularity. There is clearly a difference between DES and 3DES. But, there was not time to develop a scale of the granularity required to specify this difference during the pilot. Perhaps an alphanumeric trigraph (CS1, CS2, *etc.*) could be used for a descriptor when the number of levels required are determined. For example, perhaps a CS1 rating might be given to 3DES and SKIPJACK and a CS2 (or lower) for the others, as appropriate, 1 indicating the most computationally secure level. An arbitrary fifth graduation, CCS (Conditionally Computationally Secure), was adopted for illustration in this pilot.

Any CS rating for RC5 and RSA is conditional, which is the reason for the 5th, Conditionally Computationally Secure (CCS), rating. The keys used must be "long enough" to warrant a CS rating. In the case of RC5, as with DES, there also must be "enough" rounds. These "enough" values are a function of the best method(s) of attack as well as the state of cryptographic mathematics, processor hardware and software technology. There was not time to formulate and compute these key length and round threshold values during this limited pilot. (Street and Walker have recently suggested a three graduation scale[26] for indicating the strength of cryptography based on key length: "Weak Cryptography," applications with secret keys of 40 bits (DES, RC2, RC4), and for public key 512 bits or less; "Good Cryptography," secret key of 56 bits (typically DES), public key 512 to 1024 bits; and, "Strong Cryptography," secret key lengths in excess of 56 bits and public keys that are 1024 bits and larger.)

The Attack Times in years shown in Table 3 were derived by dividing the Attack Steps by the pilot Mtops per year (3.83×10^{16} operations per year.) Obviously, these are enormous periods of time using the comparatively small symmetrical multiprocessor (SMP), with only four processors, which was chosen for this illustration. (The age of the universe is roughly somewhere between 10^{10} and 10^{17} years.) There are larger SMPs but there is a point, as you keep adding processors in the SMP architecture, at which efficiency declines due to memory contention since all the processors use the same memory. Massive parallel processor (MPP) architectures provide each processor with its own memory, so in theory, there is no limit to the size of massively parallel machines because each processor has its own logical and physical memory. As MPP hardware and software technology advance and Mtop years become larger there may be an impressive reduction in Attack Times. Quantum computers, with their potential for breaking public key ciphers by factoring their large asymmetric keys, could be exploited to perform the factoring calculations in a few seconds that would take billions of years on today's most powerful

[25] Rivest, Ron, E-mail message of 15 June 1995, 15:17:44 EDT, Subject: Attack Steps Metric.

[26] Street, William B. and Walker, Stephen T., *Commercial Automated Key Escrow (CAKE): An Exportable Strong Encryption Alternative*, Version 2.0, National Semiconductor iPower Business Unit, Sunnyvale, CA, 4 June 1995, p 5.

classical computers.[27] If processor strength continues to double every 18 months, for every five years in the future it seems safe to assume that an attack will be either 10 times faster or 10 times cheaper than it would be today, depending on the value of time or the investment required. (A Speed Metric scale suggests itself, with graduations in processor clock cycles per bite of encryption, which was not developed for this pilot.)

Cryptographic Algorithm Metrics	DES[1]	3DES[2]	SKIPJACK	RC5[3]	RSA[4]
Key Length in Bits	56	112 [5]	80	64	1024
Attack Time in Years	1.37×10^{11}	1.25×10^{28}	2.56×10^{18}	3.61×10^{13}	2.40×10^{17}
Attack Steps	2^{56}	2^{112} (See footnote 5)	2^{80}	2^{64}	Factoring
Rounds	16	48	32	Variable 0, 1 to 255	Not Applicable
Algorithm Strength	CS[6]	CS	CS	CCS[7]	CCS[8]

Table 3. Pilot Examples of Metrics for Cryptographic Algorithms

1 Data Encryption Standard, FIPS PUB 46-2.
2 Triple DES, standard DES encryption executed three times.
3 RC stands for Ron's Code, named by the inventor, Dr. Ronald L. Rivest, Chairman of RSA.
4 RSA; is the first letter of the last names of the three collaborating creators; R.L. **R**ivest, A. **S**hamir and L.M. **A**dleman.
5 There is not complete agreement that the effective key length of 3DES is 112. An ANSI Working Group is now considering a recommendation for the use of three different keys in 3DES, which might result in an effective key length of 168.
6 CS is the abbreviation for Computationally Secure. The CS rating for DES is now questionable in certain circumstances.
7 CCS is Conditionally Computationally Secure, the conditional qualification being the key length . A CS rating for RC5 would not be correct for "short" keys lengths. RC5 accommodates keys up to 255 bits, but 64 was arbitrarily chosen because 64 seemed like a fair key length for comparison with the other symmetric algorithms in the table.
8 Similarly, a CS rating would not be justified for "short" RSA keys. Although there are 512 bit RSA applications still in use, Dr. Rivest recommends a minimum RSA key of 1024 bits.

There probably should be a time weighting system for various types of Attack Steps that was not developed during this pilot. There are still other uncertainties associated with the Attack Steps row because the number of attack steps are a function of the method of attack selected. For all but RSA, the method of attack postulated for the times shown in Table 3 is an exhaustive brute force attack, in which the adversary essentially tries all possible keys until one is found that

[27] Glanz, James, "Quantum Leap for Computers?," *Science*, Vol. 269, 7 July 1995.

decrypts the ciphertext into a known or meaningful plaintext message. The correct key could be the last one tried. The RSA Attack Time is an estimate for a successful factoring attack to discover a 1024 bit key, based on the best publicly known factoring algorithm, the Number Field Sieve (NFS) algorithm.

V. SUMMARY

The authors believe that this small sample population of cryptographic algorithms and examples of the sort of metrics that might be used to specify algorithm strength is sufficient to suggest that it may be possible to develop values for cryptographic algorithms and related technologies. They could also prove useful in specifying Common Criteria levels of assurance for cryptographic subsystems or functional areas. These metrics might also be useful for evaluating and comparing product capabilities, although there is probably a different (or additional) set of scales that could be developed for rating the strength of the cryptographic functionality of various products.

Based on the experience of this pilot, it also might be possible to develop metrics for the specification of other Information Security technologies and products.. In any case, it probably should be a joint responsibility of USG Departments or agencies to undertake, or sponsor, the further development of cryptographic algorithm metrics. Also, the development of cryptographic metrics might be an appropriate task for national or international standards organizations.

97RSAP
20 Aug 96
BU9

This page intentionally left blank.

CRYPTOGRAPHIC ALGORITHM METRICS

Appendix A

Acronyms and Definitions

10 June 1996

ACRONYMS AND DEFINITIONS

3DES Triple DES

Asymmetric A public key or two-key cryptographic algorithm. An asymmetric public key algorithm uses two related keys, a public key and a private key; the two keys have the property that, given the public key, it is computationally infeasible to derive the private key.

C^3ICM Command, Control, Communications and Intelligence Countermeasures

C^4ISR Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

CBC Cipher Block Chaining (CBC) mode - CBC is a block cipher system in which the first plain text data block is exclusive-ORed with the next plain text data block to form the next input block to the DES, thus chaining together blocks of cipher text. The chaining of cipher text blocks provides an error extension characteristic which is valuable in protecting against fraudulent data alteration. See Appendix of FIPS PUB 81.

CFB The CFB mode is a stream method of encryption in which the DES is used to generate pseudorandom bits that are exclusive-ORed with binary plain text to form cipher text. The cipher test is fed back to form the next DES input block.

CFR Code of Federal Regulations

Computationally Infeasible: - The property that a computation is theoretically achievable but is not feasible in terms of the time or resources required to perform it with the current or predicted power of computers.

Cryptography The discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof.

CRYPT-X An Australian computer software package that can be used to assess the security of newly-developed encryption algorithms.

CS Computationally Secure - A cipher is **C**omputationally **S**ecure, or strong, if it cannot be broken by systematic analysis with available resources in a short enough time to permit exploitation..

CCS Conditionally Computationally Secure - A cipher is **C**onditionally **C**omputationally **S**ecure, if the cipher could be implemented with keys that are not quite “long enough” or with not quite “enough” rounds to warrant a CS rating.

CTP Composite Theoretical Performance - A measure of computational performance given in millions of theoretical operations per second (Mtops). See Appendix B.

DEA Data Encryption Algorithm (See DES)

DES Data Encryption Standard (See FIPS PUB 46-2)

DSA Digital Signature Algorithm (DSA)

Encryption The process of changing plain text into cipher text. Verb: encrypt. Synonym: encipher.

ECB Electronic Codebook mode - The Electronic Codebook (ECB) mode [of DES] is a basic, block, cryptographic method which transforms 64 bits of input to 64 bits of output specified in FIPS PUB 46.

FIPS Federal Information Processing Standard

Gigabyte A thousand megabytes, a megabyte is a million bytes

Key A cryptographic key (key) is a parameter that determines the operation of a cryptographic function such as: (a) the transformation from plain text to cipher text and vice versa, (b) synchronized generation of keying material, (c) digital signature computation or validation.

MAC Message Authentication Code

Militarily Critical Technologies - A technology for which the technical performance parameters are at or above the minimum level necessary to ensure continuing superior performance of U.S. military systems.

MCTL Militarily Critical Technologies List

Mtops Millions of theoretical operations per second. See CTP.

OFB The Output Feedback (OFB) mode is an additive stream cipher in which errors in the cipher text are not extended to cause additional errors in the decrypted plain text. One bit in error in the cipher text causes only one bit to be in error in the decrypted plain text.

Plain text Unencrypted data.

PUB Publication

RAM Random access memory

RSA	The first letter of the last names of the collaborating creators: R. L. Rivest, A. Shamir and L.M. Adleman.
RC4 and 5	RC stands for Ron's Code, named after the inventor, Dr. Ronald L. Rivest, now Chairman of RSA.
SHA	Secure Hash Algorithm
SKIPJACK	The name of the algorithm required by the Escrow Encryption Standard (EES)
Symmetric	A secret key or one-key cryptographic algorithm
TWG	Technical Working Group
US	Unconditionally Secure - A cipher is **U**nconditionally **S**ecure if, no matter how much ciphertext is intercepted, there is not enough information in the ciphertext to determine the plaintext uniquely.[28] (This definition excludes algorithms which are subject to a plaintext-ciphertext attack and algorithms which permit the attacker to reduce the possible plaintext message to one of two values.)
U.S.	United States of America
USG	United States Government
VW	A **V**ery **W**eak cipher is one that can be broken by determining the key systematically in a short period of time (8 hours) with a small investment ($20K) in cryptanalysis resources.
W	Weak - A **W**eak cipher is one that can be broken by a brute force attack; i.e., the key can be recovered in an acceptable length of time (24 hours) with an "affordable" investment ($200K) in cryptanalytic resources by searching every possible key. A cipher also would be weak if its structure permitted a short-cut method of attack such as differential cryptanalysis.
XOR	Exclusive-OR operation - The bit-by-bit modulo-2 addition of two binary vectors of equal length.

[28] Denning, Dorothy E., *Cryptography and Data Security*, Addison-Wesley Publishing Company, Reading, Massachusetts, January 1983, p.3.

CRYPTOGRAPHIC ALGORITHM METRICS

Appendix B

Composite Theoretical Performance (CTP)

7 June 1997

TECHNICAL NOTE ON "COMPOSITE THEORETICAL PERFORMANCE" ("CTP")

Abbreviations used in this Technical Note

This appendix is an abridged extract from the Wassenaar Arrangement[29] explaining the agreed upon method for calculating the power of computer processors in terms of the Composite Theoretical Performance (CTP) for computers, expressed in a millions of theoretical operations per second (Mtops) metric, which was the metric used in this paper. The following abbreviations are used in the technical note:

"CE" "computing element" (typically an arithmetic logical unit)
FP floating point
XP fixed point
t execution time**
XOR exclusive OR
CPU central processing unit
TP theoretical performance (of a single "CE")**
"CTP" "composite theoretical performance" (multiple "CEs")**
R effective calculating rate
WL word length**
L word length adjustment
* multiply

(**Execution time 't' is expressed in microseconds, TP and "CTP" are expressed in millions of theoretical operations per second (Mtops) and WL is expressed in bits.)

Outline of "CTP" calculation method

"CTP" is a measure of computational performance given in Mtops. In calculating the "CTP" of an aggregation of "CEs" the following three steps are required:

1. Calculate the effective calculating rate R for each "CE";
2. Apply the word length adjustment (L) to the effective calculating rate (R), resulting in a Theoretical Performance (TP) for each "CE";
3. If there is more than one "CE", combine the TPs, resulting in a "CTP" for the aggregation.

Details for these steps are given in the following sections.

Note 1 For aggregations of multiple "CEs" which have both shared and unshared memory subsystems, the calculation of "CTP" is completed hierarchically, in

[29] *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Final Version of the Initial Elements, List of Dual-Use Goods and Technologies and Munitions List,* p. 58, 1 August 1996. The Wassenaar Arrangement is the successor international organization to the Coordinating Committee for Multilateral Control of Exports (COCOM)

two steps: first, aggregate the groups of "CEs" sharing memory; second, calculate the "CTP" of the groups using the calculation method for multiple "CEs" not sharing memory.

Note 2 "CEs" that are limited to input/output and peripheral functions (e.g. disk drive, communication and video display controllers) are not aggregated into the "CTP" calculation.

TECHNICAL NOTE ON "CTP"

The following table shows the method of calculating the Effective Calculating Rate R for each "CE":

Step 1: The effective calculating rate R

For "CEs" Implementing: Note Every "CE" must be evaluated independently.	Effective calculating Rate, R
XP only (R xp)	$\frac{1}{3*(t_{xp\ add})}$ if no add is implemented use: $\frac{1}{(t_{xp\ mult})}$ If neither add nor multiply is implemented use the fastest available arithmetic operation as follows: $\frac{1}{3 * t_{xp}}$ See Notes X & Z
FP only (R fp)	$\max \frac{1}{t_{fp\ add}}, \frac{1}{t_{fp\ mult}}$ See Notes X & Y
Both FP and XP (R)	Calculate both R_{xp}, R_{fp}
For simple logic processors not implementing any of the specified arithmetic operations.	$\frac{1}{3 * t_{log}}$ Where t_{log} is the execute time of the XOR, or for logic hardware not implementing the XOR, the fastest simple logic operation. See Notes X & Z
For special logic processors not using any of the specified arithmetic or logic operations.	R = R' * WL/64 Where R' is the number of results per second, WL is the number of bits upon which the logic operation occurs, and 64 is a factor to normalize to a 64 bit operation.

TECHNICAL NOTE ON "CTP"

Note W For a pipelined "CE" capable of executing up to one arithmetic or logic operation every clock cycle after the pipeline is full, a pipelined rate can be established. The effective calculating rate (R) for such a "CE" is the faster of the pipelined rate or non-pipelined execution rate.

Note X For a "CE" which performs multiple operations of a specific type in a single cycle (e.g., two additions per cycle or two identical logic operations per cycle), the execution time t is given by:

$$t = \frac{\text{cycle time}}{\text{the number of identical operations per machine cycle}}$$

"CEs" which perform different types of arithmetic or logic operations in a single machine cycle are to be treated as multiple separate "CEs" performing simultaneously (e.g., a "CE" performing an addition and a multiplication in one cycle is to be treated as two "CEs", the first performing an addition in one cycle and the second performing a multiplication in one cycle).

If a single "CE" has both scalar function and vector function, use the shorter execution time value.

Note Y For the "CE" that does not implement FP add or FP multiply, but that performs FP divide:

$$R_{fp} = \frac{1}{t_{fpdivide}}$$

If the "CE" implements FP reciprocal but not FP add, FP multiply or FP divide, then

$$R_{fp} = \frac{1}{t_{fpreciprocal}}$$

If none of the specified instructions is implemented, the effective FP rate is 0.

Note Z In simple logic operations, a single instruction performs a single logic manipulation of no more than two operands of given lengths.

In complex logic operations, a single instruction performs multiple logic manipulations to produce one or more results from two or more operands.

Note Z

Rates should be calculated for all supported operand lengths considering both pipelined operations (if supported), and non-pipelined operations using the fastest executing instruction for each operand length based on:

1. Pipelined or register-to-register operations**.** Exclude extraordinarily short execution times generated for operations on a predetermined operand or operands (for example, multiplication by 0 or 1). If no register-to-register operations are implemented, continue with (2).
2. The faster of register-to-memory or memory-to-register operations; if these also do not exist, then continue with (3).
3. Memory-to-memory.

In each case above, use the shortest execution time certified by the manufacturer.

Step 2: TP for each supported operand length WL

Adjust the effective rate R (or R') by the word length adjustment L as follows:

$$TP = R * L,$$
$$\text{where } L = (1/3 + WL/96)$$

Note The word length WL used in these calculations is the operand length in bits. (If an operation uses operands of different lengths, select the largest word length.)

The combination of a mantissa ALU and an exponent ALU of a floating point processor or unit is considered to be one "CE" with a Word Length (WL) equal to the number of bits in the data representation (typically 32 or 64) for purposes of the "CTP" calculation.

This adjustment is not applied to specialized logic processors which do not use XOR instructions. In this case TP = R.

Select the maximum resulting value of TP for:

Each XP-only "CE" (R_{xp});
Each FP-only "CE" (R_{fp});
Each combined FP and XP "CE" (R);
Each simple logic processor not implementing any of the specified arithmetic operations; and,
Each special logic processor not using any of the specified arithmetic or logic operations.

Step 3: "CTP" for aggregations of "CEs", including CPUs.

For a CPU with a single "CE",

"CTP" = TP

(for "CEs" performing both fixed and floating point operations

$TP = \max (TP_{fp}, TP_{xp})$)

"CTP" for aggregations of multiple "CEs" operating simultaneously is calculated as follows:

Note 1 For aggregations that do not allow all of the "CEs" to run simultaneously, the possible combination of "CEs" that provides the largest "CTP" should be used. The TP of each contributing "CE" is to be calculated at its maximum value theoretically possible before the "CTP" of the combination is derived.

N.B. To determine the possible combinations of simultaneously operating "CEs", generate an instruction sequence that initiates operations in multiple "CEs", beginning with the slowest "CE" (the one needing the largest number of cycles to complete its operation) and ending with the fastest "CE". At each cycle of the sequence, the combination of "CEs" that are in operation during that cycle is a possible combination. The instruction sequence must take into account all hardware and/or architectural constraints on overlapping operations.

Note 2 A single integrated circuit chip or board assembly may contain multiple "CEs".

Note 3 Simultaneous operations are assumed to exist when the computer manufacturer claims concurrent, parallel or simultaneous operation or execution in a manual or brochure for the computer.

Note 4 "CTP" values are not to be aggregated for "CE" combinations (inter)connected by "Local Area Networks", Wide Area Networks, I/O shared connections/devices, I/O controllers and any communication interconnection implemented by software.

TECHNICAL NOTE ON "CTP"

Note 5 "CTP" values must be aggregated for multiple "CEs" specially designed to enhance performance by aggregation, operating simultaneously and sharing memory,- or multiple memory/"CE"- combinations operating simultaneously utilising specially designed hardware.
This aggregation does not apply to "assemblies" described by 4.A.3.d.

$$\text{"CTP"} = TP_1 + C_2 * TP_2 + ... + C_n * TP_n,$$

where the TPs are ordered by value, with TP_1 being the highest, TP_2 being the second highest, ..., and TP_n being the lowest. C_i is a coefficient determined by the strength of the interconnection between "CEs", as follows:

For multiple "CEs" operating simultaneously and sharing memory:

$$C_2 = C_3 = C_4 = ... = C_n = 0.75$$

Note 1 When the "CTP" calculated by the above method does not exceed 194 Mtops, the following formula may be used to calculate C_i:

$$C_i = \frac{0.75}{\sqrt{m}} \qquad (i = 2, ..., n)$$

where m = the number of "CEs" or groups of "CEs" sharing access.

provided:
1. The TP_i of each "CE" or group of "CEs" does not exceed 30 Mtops;
2. The "CEs" or groups of "CEs" share access to main memory (excluding cache memory) over a single channel; and
3. Only one "CE" or group of "CEs" can have use of the channel at any given time.

N.B. This does not apply to items controlled under Category 3.

Note 2 "CEs" share memory if they access a common segment of solid state memory. This memory may include cache memory, main memory or other internal memory. Peripheral memory devices such as disk drives, tape drives or RAM disks are not included.

TECHNICAL NOTE ON "CTP"

For Multiple "CEs" or groups of "CEs" not sharing memory, interconnected by one or more data channels:

C_i = 0.75 * k_i (i = 2, ... , 32) (see Note below)
= 0.60 * k_i (i = 33, ... , 64)
= 0.45 * k_i (i = 65, ... , 256)
= 0.30 * k_i (i > 256)

The value of C_i is based on the number of "CE"s, not the number of nodes.

where k_i = min (S_i/K_r, 1), and
K_r = normalizing factor of 20 MByte/s.
S_i = sum of the maximum data rates (in units of MByte/s) for all data channels connected to the i^{th} "CE" or group of "CEs" sharing memory.

When calculating a C_i for a group of "CEs", the number of the first "CE" in a group determines the proper limit for C_i. For example, in an aggregation of groups consisting of 3 "CEs" each, the 22nd group will contain "CE"$_{64}$, "CE"$_{65}$ and "CE"$_{66}$. The proper limit for C_i for this group is 0.60.

Aggregation (of "CEs" or groups of "CEs") should be from the fastest-to-slowest; i.e.:
$TP_1 \geq TP_2 \geq \ldots \geq TP_n$, and
in the case of $TP_i = TP_{i+1}$, from the largest to smallest; i.e.:
$C_i \geq C_{i+1}$

Note The k_i factor is not to be applied to "CEs" 2 to 12 if the TP_i of the "CE" or group of "CEs" is more than 50 Mtops; i.e., C_i for "CEs" 2 to 12 is 0.75.

DEFINITION OF TERMS

IL 3 "Assembly"

IL 4 A number of electronic components (i.e., "circuit elements", "discrete components", integrated circuits, etc.) connected together to perform (a) specific function(s), replaceable as an entity and normally capable of being disassembled.

N.B.1 "Circuit element": a single active or passive functional part of an electronic circuit, such as one diode, one transistor, one resistor, one capacitor, etc.

N.B.2 "Discrete component": a separately packaged "circuit element" with its own external connections.

GTN "Basic scientific research"

Experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.

IL 4 "CE" - see "computing element"

IL 4 "Composite theoretical performance" ("CTP")

A measure of computational performance given in millions of theoretical operations per second (Mtops), calculated using the aggregation of "computing elements" ("CE"). (See Category 4, Technical Note.)

IL 4 "Computer using facility"

The end-user's contiguous and accessible facilities:

a. Housing the "computer operating area" and those end-user functions which are being supported by the stated application of the electronic computer and its related equipment; and

b. Not extending beyond 1,500 m in any direction from the centre of the "computer operating area".

N.B. "Computer operating area": the immediate contiguous and accessible area around the electronic computer, where the normal operating, support and service functions take place.

IL 4 "Computing element" ("CE")

The smallest computational unit that produces an arithmetic or logic result.

IL 4 "CTP" = see "Composite theoretical performance"

IL 4 "Datagram"

IL 5 A self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination data terminal equipment without reliance on earlier exchanges between this source or destination data terminal equipment and the transporting network.

GTN "Development"

Is related to all stages prior to serial production, such as: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, layouts.

IL 4 "Digital computer"

IL 5 Equipment which can, in the form of one or more discrete variables:

a. Accept data;

b. Store data or instructions in fixed or alterable (writable) storage devices;

c. Process data by means of a stored sequence of instructions which is modifiable; and

d. Provide output of data.

N.B. Modifications of a stored sequence of instructions include replacement of fixed storage devices, but not a physical change in wiring or interconnections.

IL 4* "Expert systems"

Systems providing results by application of rules to data which are stored independently of the "programme" and capable of any of the following:

a. Modifying automatically the "source code" introduced by the user;

b. Providing knowledge linked to a class of problems in quasi-natural language; or

c. Acquiring the knowledge required for their development (symbolic training).

IL 4 "Fast select"

IL 5 A facility applicable to virtual calls which allows a data terminal equipment to expand the possibility to transmit data in call set-up and clearing "packets" beyond the basic capabilities of a virtual call.

N.B. "Packet": a group of binary digits including data and call control signals which is switched as a composite whole. The data, call control signals and possibly error control information are arranged in a specified format.

* UK to submit revised definition.

IL 4 "Fault tolerance"

The capability of a computer system, after any malfunction of any of its hardware or "software" components, to continue to operate without human intervention, at a given level of service that provides continuity of operation, data integrity and recovery of service within a given time.

IL 4 "Global interrupt latency time"

The time taken by the computer system to recognize an interrupt due to the event, service the interrupt and perform a context switch to an alternate memory-resident task waiting on the interrupt.

IL 4 "Hybrid computer"

Equipment which can:

a. Accept data;
b. Process data, in both analogue and digital representations; and
c. Provide output of data.

IL 4 "Image enhancement"

The processing of externally derived information-bearing images by algorithms such as time compression, filtering, extraction, selection, correlation, convolution or transformations between domains (e.g., fast Fourier transform or Walsh transform). This does not include algorithms using only linear or rotational transformation of a single image, such as translation, feature extraction, registration or false coloration.

GTN "In the public domain"

GSN As it applies to the International Lists, means "technology" or "software" which has been made available without restrictions upon its further dissemination.

N.B. Copyright restrictions do not remove "technology" or "software" from being "in the public domain".

IL 4 "Local area network"

A data communication system which:

a. Allows an arbitrary number of independent "data devices" to communicate directly with each other; and
b. Is confined to a geographical area of moderate size (e.g., office building, plant, campus, warehouse).

N.B. "Data device": equipment capable of transmitting or receiving sequences of digital information.

IL 4 "Main storage"

The primary storage for data or instructions for rapid access by a central processing unit. It consists of the internal storage of a "digital computer" and any hierarchical extension thereto, such as cache storage or non-sequentially accessed extended storage.

IL 4 "Maximum Bit Transfer Rate" ("MBTR")

Of solid state storage equipment: the number of data bits per second transferred between the equipment and its controller.

Of a disk drive: the internal data transfer rate calculated as follows:

"MBTR" (bits per second) = B x R x T

where:

B = Maximum number of data bits per track available to read or write in a single revolution;

R = Revolutions per second;

T = Number of tracks which can be read or written simultaneously.

IL 4 "MBTR" - see "Maximum Bit Transfer Rate"

IL 4 "Most immediate memory"

The portion of the "main storage" most directly accessible by the central processing unit:

a. For single level "main storage", the internal storage; or

b. For hierarchical "main storage":

1. The cache storage;

2. The instruction stack; or

3. The data stack.

IL 4 "Multi-data-stream processing"

The "microprogramme" or equipment architecture technique which permits simultaneous processing of two or more data sequences under the control of one or more instruction sequences by means such as:

a. Single Instruction Multiple Data (SIMD) architectures such as vector or array processors;

b. Multiple Single Instruction Multiple Data (MSIMD) architectures;

c. Multiple Instruction Multiple Data (MIMD) architectures, including those which are tightly coupled, closely coupled or loosely coupled; or

d. Structured arrays of processing elements, including systolic arrays.

IL 4 "Network access controller"

IL 5 A physical interface to a distributed switching network. It uses a common medium which operates throughout at the same "digital transfer rate" using arbitration (e.g., token or carrier sense) for transmission. Independently from any other, it selects data packets or data groups (e.g., IEEE 802) addressed to it. It is an assembly that can be integrated into computer or telecommunications equipment to provide communications access.

IL 4 "Neural computer"

A computational device designed or modified to mimic the behaviour of a neuron or a collection of neurons, i.e., a computational device which is distinguished by its hardware capability to modulate the weights and numbers of the interconnections of a multiplicity of computational components based on previous data.

IL4 "Object code" (or object language)

IL5 "Object code" (or object language): An equipment executable form of a convenient expression of one or more processes ("source code" (or source language)) which has been converted by a programming system.

IL 4 "Optical computer"

A computer designed or modified to use light to represent data and whose computational logic elements are based on directly coupled optical devices.

IL 4 "Principal element"

An element is a "principal element" when its replacement value is more than 35% of the total value of the system of which it is an element. Element value is the price paid for the element by the manufacturer of the system, or by the system integrator. Total value is the normal international selling price to unrelated parties at the point of manufacture or consolidation of shipment.

GTN "Production"

Means all production stages, such as: product engineering, manufacture, integration, assembly (mounting), inspection, testing, quality assurance.

IL 2 "Programme"

IL 4 A sequence of instructions to carry out a process in, or convertible into,

IL 5 a form executable by an electronic computer.

IL 2 "Real time processing"

IL 4 The processing of data by a computer system providing a required level of service, as a function of available resources, within a guaranteed response time, regardless of the load of the system, when stimulated by an external event.

GTN "Required"

As applied to "technology", refers to only that portion of "technology" which is peculiarly responsible for achieving or exceeding the embargoed performance levels, characteristics or functions. Such "required" "technology" may be shared by different products.

IL 3 "Signal processing"

IL 4 The processing of externally derived information-bearing signals by

IL 5 algorithms such as time compression, filtering, extraction, selection, correlation, convolution or transformations between domains (e.g., fast Fourier transform or Walsh transform).

All "Software"

ILs A collection of one or more "programmes" or "microprogrammes" fixed in any tangible medium of expression.

IL 4 "Source code" (or source language)

A convenient expression of one or more processes which may be turned by a programming system into equipment executable form ("object code" (or object language)).

IL 4 "Sputtering"

An overlay coating process wherein positively charged ions are accelerated by an electric field towards the surface of a target (coating material). The kinetic energy of the impacting ions is sufficient to cause target surface atoms to be released and deposited on the substrate.

N.B. Triode, magnetron or radio frequency sputtering to increase adhesion of coating and rate of deposition are ordinary modifications of the process.

IL 4 "Systolic array computer"

A computer where the flow and modification of the data is dynamically controllable at the logic gate level by the user.

GTN "Technology"

Specific information necessary for the "development", "production" or "use" of a product. The information takes the form of "technical data" or "technical assistance". Embargoed "technology" is defined in the General Technology Note and in the International Industrial List.

N.B.1 "Technical data" may take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories.

N.B.2 "Technical assistance" may take forms such as instruction, skills, training, working knowledge, consulting services. "Technical assistance" may involve transfer of "technical data".

IL 4 "Terminal interface equipment"

Equipment at which information enters or leaves the telecommunication system, e.g., telephone, data device, computer, facsimile device.

IL 4 "Three dimensional Vector Rate"

The number of vectors generated per second which have 10 pixel poly line vectors, clip tested, randomly oriented, with either integer or floating point X-Y-Z coordinate values (whichever produces the maximum rate).

IL 4 "Two dimensional Vector Rate"

The number of vectors generated per second which have 10 pixel poly line vectors, clip tested, randomly oriented, with either integer or floating point X-Y coordinate values (whichever produces the maximum rate).

GTN "Use"

Operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing.

IL 4 "User-accessible programmability"
IL 5 The facility allowing a user to insert, modify or replace "programmes"
IL 6 by means other than:

a. A physical change in wiring or interconnections; or
b. The setting of function controls including entry of parameters.

IL 4 Vector Rate - See "Two dimensional Vector Rate"
"Three dimensional Vector Rate".