Invited paper

Cryptography - A Selective Survey (*)

James L. Massey
Institute for Signal and Information Processing
Swiss Federal Institute of Technology
Zurich, Switzerland

Abstract. Cryptography has two goals (secrecy and/or authenticity) and the security that it affords can be of two kinds (theoretical or practical); this implies a natural four-fold division of cryptography that is adopted in this paper. Shannon's theory of theoretical secrecy is presented via a combinatorial approach. A similar approach is used to present Simmons'theory of theoretical authenticity. Practical security rests on the foundation of one-way functions and their variants. These functions are described, and illustrations are given of how they can be used to obtain practical secrecy and/or practical authenticity. Both private-key and public-key cryptographic methods are treated within a common analytical framework.

1. INTRODUCTION

The traditional goal of the communications engineer is to ensure that the message delivered to the destination is the same message as that originally produced by the information source. The enemy is noise. The cryptographer by contrast has two distinct goals: secrecy and/or authenticity. He may seek to ensure that the message is intelligible only to the intended recipient - the enemy is the "eavesdropper" who overhears the transmitted signals. He may seek instead (or also) to ensure that the identity of the sender and the integrity of the message can be unmistakably verified by the recipient - the enemy is the "spoofer" who can originate, or tamper with, transmitted signals.In fact, it is a fairly recent realization that secrecy and authenticity are quite distinct goals. In classical or private-key cryptography these two concepts were closely intertwined. Secrecy depended on the message being unintelligible to any recipient who did not know the secret key; authenticity depended on the inability of anyone without knowledge of the secret key to produce a cryptogram that would decipher to an intelligible message. It was only with the introduction of public-key cryptography by Diffie and Hellman (1976) that it became clear that secrecy and authenticity did not always go hand-in-hand.

The first comprehensive mathematical treatment of secrecy systems was given by Shannon (1949). We shall follow Shannon's lead in distinguishing between two types of cryptographic security, "theoretical" or "practical" to use Shannon's terminology, but we shall widen their usage to include authenticity as well as secrecy. *Theoretical security* means that security which the cryptographic system provides against an enemy who has unlimited computational resources available to him. *Practical security* means that provided against an enemy with finite computational resources. A system is theoretically secure if it is impossible to break regardless of how much effort the enemy cryptanalyst expends. A system is practically secure if its breaking requires a computational effort beyond this enemy's means.

The first half of this paper is concerned with the theoretical security of cryptographic systems. Shannon's (1949) theory of theoretical secrecy is described via a combinatorial approach. A similar combinatorial approach is used to outline some salient features of the still-developing theory of theoretical authenticity.

(*) Opening lecture to the "1985 International Tirrenia Workshop on Digital Communications".

The second half of this paper treats the practical security of cryptographic systems. To this end, we enlarge Diffie and Hellman's (1976) catalog of one-way functions and their variates so as to be able to treat public-key systems and private-key systems within a common framework. With the introduction of each such species of one-way functions, we give illustrations showing how such a function can be used to provide practical secrecy and/or authenticity.

2. THEORETICAL SECRECY

Shannon's (1949) model of a general secrecy system is shown in Fig. 1. We shall assume that the *cryptogram* Y is a binary sequence of length N and that the *key* Z is a binary sequence of length K. We shall be less specific in general about the form of the *plaintext message* X, assuming only that there are 2^M different valid values of X (so that, at least in principle, X could be coded into a binary sequence of length M) and we shall let A denote this set of valid messages.

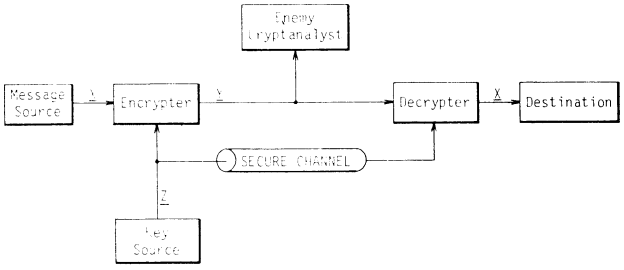

Fig. 1 - Shannon's Model of a General Secrecy System

Shannon (1949) used the term *perfect secrecy* to describe the situation when the enemy cryptanalyst in Fig. 1 can do no better than to guess X without bothering to study the cryptogram Y, i.e., when X and Y are statistically independent. It is surprisingly easy (in principle) to realize perfect secrecy systems.

Example 1: Suppose that A consists of 2^M binary sequences of length n, where of course $n \geq M$. [In binary-coded English text, $n \approx 5M$ would be typical.] Consider the so-called "one-time pad" system in which Z has length $K = n$, all 2^n keys are equiprobable, and

$$Y = X \oplus Z \tag{1}$$

where $\oplus$ denotes component-wise addition modulo 2. For every $x \in A$ and every binary sequence y of length n, it follows from (1) that there will be exactly one key z that will cause x to be encrypted into y.

Thus $P(Y = y \mid X = x) = 2^{-n}$ independently of x and hence X and Y are statistically independent. The system gives perfect secrecy! That the enemy cryptanalyst might as well guess X without looking at Y is perhaps more obvious to the communications engineer after noting that (1) is equivalent to saying that Y is what is received when X is transmitted through a binary symmetric channel (BSC) with crossover probability 1/2, i.e., with zero capacity.

The one-time pad requires 1 bit of secret key for each binary digit of the plaintext. If the 2^M different plaintexts were equally likely and if A were the set of binary sequences of length M (as would be the case for perfect data compression of some information source), then the one-time pad requires 1 bit of secret key for each bit of plaintext information. It is almost obvious, and Shannon (1949) has proved, that this is the minimum amount of secret key in any perfect secrecy system.

It should be noted that Shannon's perfect secrecy assumes that the enemy cryptanalyst is limited to a *ciphertext-only* attack and, moreover, that the only ciphertext which this enemy knows is the single cryptogram that he is trying to break. [Actually, Shannon assumed that the secret key would be changed after each encryption or, equivalently,, that what we are considering as a single plaintext message X is actually the concatenation of all messages that are enciphered before the key is changed.] It is instructive to extend Shannon's theory to the case where the enemy cryptanalyst can make a *known-plaintext* attack. We shall say that this enemy can make a known-plaintext attack of *order* L in case that he knows L valid and distinct plaintext-cryptogram pairs for the key Z in effect for the cryptogram Y that he wishes to decipher. [Note that an order 0 known-plaintext attack is a ciphertext-only attack.] Of course, if Y happens to be one of the L known cryptograms, this enemy can certainly decipher Y, and otherwise he can be sure that X is not one of the L known plaintexts; at best he can say no more. It thus seems natural to say that the cryptosystem provides *perfect secrecy against an order* L *known-plaintext attack* if (1) it provides such perfect secrecy for an order $L - 1$ attack and (2) for each specification of the distinct known plaintext-cryptogram pairs $(x_1, y_1), (x_2, y_2), \ldots, (x_L, y_L)$, the enemy cryptanalyst can do no better than to guess at X without further consideration of Y when he is told that Y is not one of the L known cryptograms.

This definition is equivalent to saying that the system offers perfect secrecy against an order L known-plaintext attack just when for every i, $0 \leq i \leq L$, and for every choice of $(x_1, y_1), (x_2, y_2), \ldots, (x_i, y_i)$, as pairs consistent with at least one key, X and Y are statistically independent when all probabilities are conditioned on the event that the key Z be consistent with these L chosen plaintext-cryptogram pairs. We now show that it is easy (in principle) to construct a system that yields perfect secrecy against the extreme of a known-plaintext attack of order $2^M - 2$ [if the enemy knows $2^M - 1$ distinct plaintext-cryptogram pairs, he can always decrypt Y].

Example 2: Again suppose that the set of plaintexts A consists of 2^M binary sequences of length n, where of course $n \geq M$. Let B denote the set of all 2^n binary sequences so that $A \subset B$. Consider the "symmetric group" S of all $(2^n)!$ substitutions on B, i.e., all the invertible mappings from B to itself, and suppose that the key Z is used to choose one of these substitutions as the enciphering function so that each of the $(2^n)!$ substitutions is equally likely. The key length K then is

$$K = \lceil \log_2(2^n!) \rceil \approx \approx n2^n . \quad (2)$$

For any choice of $(x_1, y_1), (x_2, y_2), \ldots, (x_i, y_i)$, where $x_1, x_2, \ldots, x_i$ are all distinct as also are $y_1, y_2, \ldots, y_i$, there are exactly $(2^n - i)!$ substitutions in S for which these i pairs are valid plaintext-cryptogram pairs; moreover, these are *all* the invertible functions from $B - \{x_1, \ldots, x_i\}$ to $B - \{y_1, \ldots, y_i\}$. Thus, for every $x \notin B - \{x_1, \ldots, x_i\}$ and every $y \notin B - \{y_1, \ldots, y_i\}$,

$$P(Y = y \mid X = x, Z \text{ consistent with } (x_1, y_1), \ldots, (x_i, y_i)) = \frac{1}{2^n - i} , \quad (3)$$

which shows that the system provides perfect secrecy.

We see from (2) that to provide perfect secrecy against a known-plaintext attack of order $2^n - 2$ our proposed system requires about 2^n bits of key for each binary digit of the plaintext! In fact, we can adapt Shannon's proof for the ciphertext-only situation to show that our proposed system uses the minimum amount of secret key when $M = n$ and the 2^M plaintext messages are equally likely. The "trick" is just to note that if the system gives perfect secrecy against a known-plaintext attack of order $2^n - 2$, then the sequence of all 2^M distinct plaintext messages, in any order, is equally likely to result in all possible sequences of the 2^M distinct corresponding cryptograms. Thus, the sequence of cryptograms only is useless to the enemy cryptographer in determining the order of the plaintext messages. But there are $(2^M)!$ such orderings, and hence $\log_2(2^M!)$ bits of information can be sent with perfect secrecy if the enemy can observe only ciphertext.

Thus, Shannon's lower bound for perfect secrecy of one bit of key per bit of information in the plaintext demands that

$$K \geq \lceil \log_2(2^M!) \rceil . \quad (4)$$

By a similar argument, it follows that any cryptosystem that gives perfect secrecy against a known-plaintext attack of order L must have a key size satisfying

$$K \geq \lceil \log_2 \prod_{i=0}^{L} (2^M - i) \rceil \approx \approx (L + 1)M . \quad (5)$$

We have seen that the lower bound of (5) is attainable when $L = 0$ and $L = 2^M - 2$, the extreme values; presumably one can achieve, or come very close to, this lower bound for all L, but we will not try to prove this. Our aim is merely to show that perfect secrecy against a known-plaintext attack requires an enormous amount of secret key, this amount increasing linearly with the number of known plaintext-cryptogram pairs.

3. THEORETICAL AUTHENTICITY

The theory of authenticity is a recent and still incomplete one. The initial study appears to be that of Gilbert, MacWilliams and Sloane (1974), extended later by Fak (1979). Simmons (1981, 1984 and 1985) has placed this work in a more general setting and developed a more systematic theory. Our treatment here will be in the spirit of Simmons' work, but we have altered his approach somewhat to enhance the parallels between the theory of authenticity and Shannon's theory of secrecy.

Our model of a general authenticity system is shown in Fig. 2 in which we have retained as far as possible the notation and terminology that we used with Fig. 1. The crucial difference between Figs. 1 and 2 is that it is now the enemy cryptanalyst who chooses the "cryptogram" $\hat{Y}$ that reaches the destination. We have used a dotted line in Fig. 2 to indicate that we will not always assume that this enemy knows the legitimate cryptogram Y.

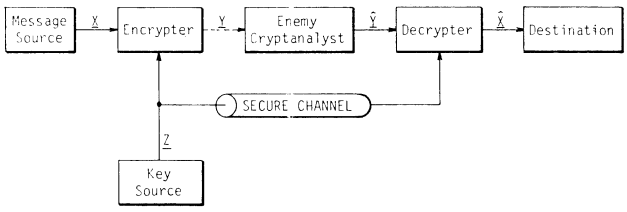

Fig. 2 - Model of a General Authenticity System

Simmons distinguishes between two different types of fraud the enemy cryptanalyst might seek to perpetrate, viz. impersonation and substitution. By *impersonation*, he means that, without knowledge of Y (and indeed there may not even be a valid cryptogram Y), the enemy tries to form a signal $\hat{Y}$ that is a valid cryptogram for the key Z in effect. The probability, P_I, of successful impersonation is the measure of the enemy's success. Note that impersonation succeeds even when the enemy happens to form the legitimate cryptogram Y, in case there happens to be such a cryptogram. By *substitution*, Simmons means that, knowing the valid cryptogram Y, the enemy tries to form a signal $\hat{Y}$, different from Y, that is also a valid cryptogram. The enemy's success is measured by the probability, P_S, of a successful substitution.

Let B denote the set of all possible cryptograms, i.e., the set of all 2^N binary sequences of length N. By analogy to the terminology for secrecy systems, we shall use the term "perfect" to describe authenticity systems where the enemy can do no better than to choose $\hat{Y}$ randomly and uniformly from B (with of course the restriction that $\hat{Y} \neq Y$ when the enemy is to attempt a substitution). A paradox arises, however. Suppose that there is no redundancy in the system, i.e., that $N = M$ so that every binary sequence of length N is a valid cryptogram for every key. The enemy cannot avoid succeeding in either impersonation or substitution, i.e., $P_I = 1$ or $P_S = 1$, regardless of his strategy. But he can nonetheless do no better than random guessing of $\hat{Y}$ since this too always succeeds.

Thus, we are forced to say that the authenticity system is "perfect" even though it provides no protection against fraud whatsoever! In fact, we see in general that uniform random guessing will yield

$$P_I = 2^M/2^N = 2^{M-N} \tag{6}$$

or

$$P_S = (2^M - 1)/(2^N - 1) \tag{7}$$

for impersonation or substitution, respectively. Thus, "perfect" systems will indeed provide good protection against fraud when and only when $N - M$ is large, i.e., when there is much redundancy in the system. Hence, we shall say that an authenticity system provides *perfect type-(N, M) protection* against impersonation or substitution when the enemy cryptanalyst can do no better than the random guessing performance (6) or (7), respectively.

Example 3: The one-time pad of Example 1 with $K = N$ has the property that, for any choice $X = x$ of plaintext, the cryptogram Y is equally likely to be any of the $2^N = 2^n$ sequences in B. Thus an enemy seeking to impersonate can do no better (nor worse) than (6) - the system provides perfect type-(N, M) security against impersonation. If the enemy knows a valid cryptogram y, however, this reduces the number of possible keys Z consistent with $Y = y$ to 2^M as there are 2^M possibilities for X in (1). By first guessing one of these keys then using it to form a cryptogram $\hat{Y}$ (different from Y), the enemy's probability for successful substitution will satisfy $P_S \geq 2^{-M}$ and hence will certainly exceed (7) if $N \geq 2M$. But the enemy may be able to do much better if the set A of plaintexts has special structure. For instance, if A is the set of codewords in an (N, M) linear block code, he can add an arbitrary non-zero codeword x' to the known cryptogram y to form $\hat{Y} = y \oplus x' = x \oplus x' \oplus Z$. Because $x \oplus x'$ is another codeword, $\hat{Y}$ is a valid cryptogram and hence $P_S = 1$. In this case, the one-time pad offers no security whatsoever against substitution.

The following example illustrates a system that provides perfect protection against impersonation but no secrecy whatsoever.

Example 4: Suppose that A is the set of binary sequences of length M and that the "cryptogram" Y is just the concatenation of the plaintext X with the key Z, i.e., $Y = (X, Z)$. Note that $N = M + K$. We can consider Z to be the "signature" that the sender appends to his message. Without knowing Y, the enemy can do no better than to choose an arbitrary plaintext and guess at the signature Z. Thus (6) holds and the system provides perfect type-(N, M) security against impersonation. However, it clearly offers no protection against substitution.

The next example illustrates an authenticity system that provides perfect protection against substitution.

Example 5: Suppose that the plaintext message X is a single binary digit, i.e., $M = 1$. Consider the set of all $2^N(2^N - 1)/2$ distinct unordered pairs $\{y_0, y_1\}$ of binary sequences of length N. Suppose that the key Z is used to choose one of these pairs for the enciphering function in the manner that Y is the lexicographically first of the pair when $X = 0$ and Y is the other element of the pair when $X = 1$. The key length then, assuming $N > 1$, is

$$K = \lceil \log_2 2^N(2^N - 1)/2 \rceil = 2N - 1. \tag{8}$$

The system clearly provides perfect type-$(N, 1)$ protection against impersonation. Moreover, knowing a valid cryptogram y, the enemy cryptographer can do no better than to guess the single other valid cryptogram randomly from $B - \{y\}$. Thus, the system also offers perfect type-$(N, 1)$ protection against substitution. This system also provides perfect secrecy against a ciphertext-only attack, but a single bit of key would have sufficed to achieve this perfect secrecy!

Before developing the theory of authenticity further, we generalize the above definitions as follows. We shall say that the enemy cryptanalyst makes a *spoofing attack of order L* (where $0 \leq L < 2^M$) in the case where he knows L distinct valid cryptograms for the key Z for which he seeks to form a fraudulent cryptogram. The enemy succeeds just when $\hat{Y}$ is a valid cryptogram for this key and is not one of the L already known cryptograms. If the enemy randomly and uniformly chooses $\hat{Y}$ from the remaining $2^N - L$ elements of B, his success probability is

$$P_{SL} = (2^M - L)/(2^N - L). \tag{9}$$

[Notice that an impersonation attempt is a spoofing attack of order 0 and that a substitution attempt is a spoofing attack of order 1.] We shall say that an authenticity system provides *perfect type (N, M) protection against a spoofing attack of order L* when the enemy can achieve a success probability P_{SL} no better than (9). Equivalently, letting B_z denote the subset of B consisting of the 2^M valid cryptograms when $Z = z$, we can say that the system gives perfect protection against a spoofing attack of order L if and only if

$$P(y_{L+1} \in B_Z \mid y_i \in B_Z;\ 1 \leq i \leq L) = \\ = (2^M - L)/(2^N - L) \tag{10}$$

for all choices of $y_1, y_2, \ldots, y_{L+1}$ as distinct elements of B. This makes it clear that the probability distribution on X plays no role in determining whether the authenticity system is perfect, as the distribution for Z completely determines that for B_Z.

In our treatment of authenticity systems, we have tacitly been using an assumption that we now make explicit, namely, that the *encipherment is deterministic*. In other words, we assume that there is a function f such that $Y = f(X, Z)$ or, equivalently, that $\#(B_z) = 2^M$ for all keys z where $\#(.)$ denotes the cardinality of the indicated set. If the encipherment is random so that at least one plaintext x may encipher as two or more valid cryptograms under the same key z, then there will be an average of more than $2^M - L$ valid cryptograms that do not decipher to the same plaintext as any of the L known cryptograms. Thus even random guessing will do better than (9). In fact

(6), (7) and (9) hold for random guessing when and only when the enciphering is deterministic.

Recall that there are 2^K possible keys Z. However, as illustrated in Examples 2 and 5, we do not insist that all possible keys actually be used, i.e., that all possible keys have non-zero probability. We shall use the term an *allowed* key to mean a key z with $P(Z = z) > 0$. We now can state our first major result for theoretical authenticity.

Proposition 1: An authenticity system with equiprobable allowed keys provides perfect type-(N, M) protection against a spoofing attack of order L if and only if $n(y_1, y_2, \ldots, y_{L+1})$, the number of allowed keys z such that $y_1, y_2, \ldots, y_{L+1}$ are all cryptograms for the key z, is the same number for all choices of $y_1, y_2, \ldots, y_{L+1}$ as distinct element of B.

To prove this proposition, we first note that the assumption of equiprobable allowed keys implies

$$P(y_{L+1} \in B_Z \mid y_i \in B_Z;\ 1 \le i \le L) = \frac{n(y_1, \ldots, y_L, y_{L+1})}{n(y_1, \ldots, y_L)}. \tag{11}$$

Suppose that the system is perfect. Then (10) requires that the right side of (11) must have the same value for all choices of $y_1, \ldots, y_L, y_{L+1}$ as distinct elements of B. But $n(y_1, \ldots, y_{L+1})$ is a symmetric function of its arguments.

This implies from (11) that if $y_1, \ldots, y_{L+1}$ and $y_1', \ldots, y_{L+1}'$ can be reordered to differ only in their last element, then $n(y_1, \ldots, y_{L+1}) = n(y_1', \ldots, y_{L+1}')$.

But a sequence $y_1'', \ldots, y_{L+1}''$ that differs from $y_1, \ldots, y_{L+1}$ in the last two elements after reordering will differ from some such $y_1', \ldots, y_{L+1}'$ only in the last element after reordering.

Thus $n(y_1, \ldots, y_{L+1}) = n(y_1'', \ldots, y_{L+1}'')$ also.

An iteration of this argument shows that every choice of $y_1, \ldots, y_{L+1}$ as distinct elements of B must yield the same value of $n(y_1, \ldots, y_{L+1})$.

Conversely, suppose that there is an integer n_{L+1} such that $n(y_1, \ldots, y_{L+1}) = n_{L+1}$ for all choices of $y_1, \ldots, y_{L+1}$ as distinct elements of B. Because any one key z such that $\{y_1, \ldots, y_L\} \in B_z$ is such that $\{y_1, \ldots, y_L, y\} \in B_z$ for exactly $2^M - L$ choices of y not in $\{y_1, \ldots, y_L\}$, it follows that

$$(2^M - L)\, n(y_1, \ldots, y_L) = \sum_{y \notin \{y_1, \ldots, y_L\}} n(y_1, \ldots, y_L, y).$$

By hypothesis, each of the $2^N - L$ terms in the sum on the right equals n_{L+1} so that

$$n(y_1, \ldots, y_L) = \frac{2^N - L}{2^M - L} n_{L+1} \tag{12}$$

and thus $n(y_1, \ldots, y_L)$ also has a constant value, say n_L, for all choices of $y_1, \ldots, y_L$ as distinct elements of B. But (11) and (12) combine to give (10), which proves that the authenticity system is perfect.

Note that our proof of Proposition 1 actually showed that the constancy of $n(y_1, \ldots, y_{L+1})$ implies the constancy of $n(y_1, \ldots, y_i)$ for $1 \le i \le L$ as well. Thus, we have established the following fact.

Proposition 2: An authenticity system with equiprobable allowed keys that provides perfect type-(N, M) protection against a spoofing attack of order L also provides such perfect protection against spoofing attack of order i for $0 \le i < L$.

It follows from iteration of (12) that, in a perfect system with equiprobable keys,

$$n_0 = \frac{2^N (2^N - 1) \ldots (2^N - L)}{2^M (2^M - 1) \ldots (2^M - L)} n_{L+1} \tag{13}$$

where n_i is the number of allowed keys consistent with every choice of $y_1, y_2, \ldots, y_i$ as distinct elements of B, so that n_0 is just the total number of allowed keys. But $L < 2^M$ and $n_{L+1} \ge 1$; thus taking logarithms in (13) gives the following bound on key size.

Proposition 3: An authenticity system with equiprobable allowed keys that provides perfect type-(N, M) protection against a spoofing attack of order L must have a key size K satisfying

$$K \ge \left\lceil \sum_{i=0}^{L} \log_2 \frac{2^N - i}{2^M - i} \right\rceil \approx \approx (L + 1)(N - M). \tag{14}$$

Remark: In fact *the bound* of Proposition 3 *holds regardless of whether the allowed keys are equally likely* since, in a perfect system, $n(y_1, \ldots, y_{L+1}) \ge 1$ for all choices of $y_1, \ldots, y_{L+1}$ as distinct elements of B and this is enough to ensure that the number of allowed keys must be at least as great as the right side of (13) when $n_{L+1} = 1$.

The "signature" system of Example 4 has key size $K = N - M$ and thus meets the bound (14) with equality for perfect protection against impersonation ($L = 0$).

[The $M = 1$ bit of plaintext system of Example 5 also meets the bound (14) with equality for perfect protection against substitution ($L = 1$) as can be seen from (8)].

It is easy to meet the bound (14) with equality at the other extreme $L = 2^M - 1$.

Example 6: Consider the $\binom{2^N}{2^M}$ possible sets of 2^M distinct elements of B. Consider an authenticity system with $n_0 = \binom{2^N}{2^M}$ allowed keys where each one of these sets is the set of cryptograms for one key.

The mapping from plaintexts to cryptograms can be chosen in any convenient or desirable way. If the allowed keys are equally likely, it follows from Proposition 1 that the system offers perfect type-(N, M) protection against a spoofing attack of order $L = 2^M - 1$. We may choose the key size K to be

it is easy to generate algorithms E_z and D_z that easily compute f_z and f_z^{-1}, respectively, but (2) even when given without computational cost the values $f_z(x)$ for any presented values of x, it is computationally unfeasible for virtually all y in the domain of f_z to find $f_z^{-1}(y)$ without knowledge of z. Note that an invertible trapdoor one-way function is also a keyed one-way function, since one may use the algorithm E_z to compute for one's self the values $f_z(x)$ for any desired arguments x. The converse is not true, however, because to be told $f_z(x)$ for any desired arguments x is not equivalent to knowing an algorithm for computing f_z.

It should be obvious that a keyed one-way function can be used to make a private key cryptosystem that is computationally secure against a chosen-plaintext attack, and indeed conversely. The family of functions f_z constituting the data encryption standard (DES) published by the U.S. National Bureau of Standards (1977) seems to be such a keyed one-way function; the DES key z is a binary sequence of length 64. [In fact it is somewhat remarkable that no one has yet announced a successful chosen-plaintext attack against DES as the number of keys, $2^{56} \approx 10^{17}$, is only a trifle too many to thwart an exhaustive cryptanalysis.] Our point to be made here in closing is that the conceptual clarity provided by one-way function concepts need not be confined to public key cryptography alone, we can and probably should use these concepts to *enhance understanding of private key cryptography as well.*

REFERENCES

[1] Diffie, W. and Hellman, M.E., *New Directions in Cryptography*, IEEE Trans. Info. Th., IT-22 (1976), 644-654.

[2] Fak, V., *Repeated Use of Codes which Detect Deception*, IEEE Trans. Info. Th., IT-25, (1978), 233-234.

[3] Gilbert, E., MacWilliams, F.J., and Sloane, N.J.A., *Codes which Detect Deception*, Bell Sys. Tech. J., 53 (1974), 405-424.

[4] Massey, J.L. and Rueppel, R., *Telecommand Up-Link Signature System*, Preliminary Report to European Space Technology and Engineering Center (1984).

[5] Merkle, R. and Hellman, M.E., *Hiding Information and Signatures in Trapdoor Knapsacks*, IEEE Trans. Info. Th., IT-24 (1978), 525-530.

[6] National Bureau of Standards, Data Encryption Standard, FIPS Publ. 46 (1977).

[7] Pohlig, S.C. and Hellman, M.E., *An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance*, IEEE Trans. Info. Th., IT-24 (1978), 106-110.

[8] Rivest, R.L., Shamir, A. and Adleman, L., *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Comm. ACM, 21 (1978), 120-126.

[9] Shamir, A., *A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Knapsack*, Proc. 23rd Ann. Symp. Foundations Comp. Sci. (1982), 145-152. Also appears in IEEE Trans. Info. Th., IT-30 (1984), 699-704.

[10] Shannon, C.E., *Communication Theory of Secrecy Systems*, Bell. Sys. Tech. J., 28 (1949), 656-715.

[11] Simmons, G.J., *A Preliminary Report on a Theory of Authentication*, Proc. Nat. Elec. Conf. (1981), 315-318.

[12] Simmons, G.J., *Message Authentication: A Game on Hypergraphs*, Proc. 15th Southeastern Conf. Combinatorics, Graph Th. and Computing (1984).

[13] Simmons, G.J., *Authentication Theory/Coding Theory*, Preliminary Manuscript (1985).