An Overview of Public Key Cryptography

Martin E. Hellman

With a public key cryptosystem, the key used to encipher a message can be made public without compromising the secrecy of a different key needed to decipher that message.

I. COMMERCIAL NEED FOR ENCRYPTION

Cryptography has been of great importance to the military and diplomatic communities since antiquity but failed, until recently, to attract much commercial attention. Recent commercial interest, by contrast, has been almost explosive due to the rapid computerization of information storage, transmission, and spying.

Telephone lines are vulnerable to wiretapping, and if carried by microwave radio, this need not entail the physical tapping of any wires. The act becomes passive and almost undetectable. It recently came to light that the Russians were using the antenna farms on the roofs of their embassy and consulates to listen in on domestic telephone conversations, and that they had been successful in sorting out some conversations to Congressmen.

Human sorting could be used, but is too expensive because only a small percentage of the traffic is interesting. Instead, the Russians automatically sorted the traffic on the basis of the dialing tones which precede each conversation and specify the number being called. These tones can be demodulated and a microprocessor used to activate a tape recorder whenever an "interesting" telephone number (one stored in memory) is detected. The low cost of such a device makes it possible to economically sort thousands of conversations for even one interesting one.

This work was supported in part under NSF Grant ENG 10173.
The author is with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305.

This problem is compounded in remote computing because the entire "conversation" is in computer readable form. An eavesdropper can then cheaply sort messages not only on the basis of the called number, but also on the content of the message, and record all messages which contain one or more keywords. By including a name or product on this list, an eavesdropper will obtain all messages from, to, or about the "targeted" person or product. While each fact by itself may not be considered sensitive, the compilation of so many facts will often be considered highly confidential.

It is now seen why electronic mail must be cryptographically protected, even though almost no physical mail is given this protection. Confidential physical messages are not written on postcards and, even if they were, could not be scanned at a cost of only $1 for several million words.

II. THE COST OF ENCRYPTION

Books about World War II intelligence operations make it clear that the allies were routinely reading enciphered German messages. The weakness of the Japanese codes was established by the Congressional hearings into the Pearl Harbor disaster, and while it is less well publicized, the Germans had broken the primary American field cipher.

If the major military powers of World War II could not afford secure cryptographic equipment, how is industry to do so in its much more cost-conscious environment?

0148-9615/78/1100-0024$00.75

Encryption is a special form of computation and, just as it was impossible to build good, inexpensive, reliable, portable computers in the 1940's, it was impossible to build good (secure), inexpensive, reliable, portable encryption units. The scientific calculator which sells for under $100 today would have cost on the order of a million dollars and required an entire room to house it in 1945.

While embryonic computers were developed during the war (often for codebreaking), they were too expensive, unreliable, and bulky for field use. Most computational aids were mechanical in nature and based on gears. Similarly, all of the major field ciphers employed gear-based devices and, just as Babbage's failure indicates the difficulty of building a good computer out of gears, it is also difficult to build a good cryptosystem from gears. The development of general-purpose digital hardware has freed the designers of cryptographic equipment to use the best operations from a cryptographic point of view, without having to worry about extraneous mechanical constraints.

As an illustration of the current low cost of encryption, the recently promulgated national Data Encryption Standard (DES) can be implemented on a single integrated circuit chip, and will sell in the $10 range before long. While some have criticized the standard as not being adequately secure [1], this inadequacy is due to political considerations and is not the fault of insufficient technology.

III. KEY DISTRIBUTION AND PUBLIC KEY SYSTEMS

While digital technology has reduced the cost of encryption to an almost negligible level, there are other major problems involved in securing a communication network. One of the most pressing is key distribution, the problem of securely transmitting keys to the users who need them.

The classical solution to the key distribution problem is indicated in Fig. 1. The key is distributed over a secure channel as indicated by the shielded cable. The secure channel is not used for direct transmission of the plaintext message P because it is too slow or expensive.

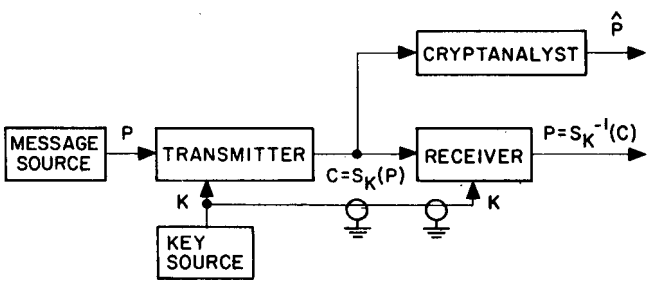


Fig. 1. Conventional Cryptographic System.

The military has traditionally used courier service for distributing keys to the sender and receiver. In commercial systems registered mail might be used. Either way, key distribution is slow, expensive, and a major impediment to secure communication.

Keys could be generated for each possible conversation and distributed to the appropriate users, but the cost would be prohibitive. A system with even a million subscribers would have almost 500 billion possible keys to distribute. In the military, the chain of command limits the number of connections, but even there, key distribution has been a major problem. It will be even more acute in commercial systems.

It is possible for each user to have only one key which he shares with the network rather than with any other user, and for the network to use this as a master key for distributing conversation specific keys [2], [3]. This method requires that the portion of the network which distributes the keys (known as the key distribution center or node) be trustworthy and secure.

Diffie and Hellman [4] and independently Merkle [5] have proposed a radically different approach to the key distribution problem. As indicated in Fig. 2, secure communication takes place without any prearrangement between the conversants and without access to a secure key distribution channel. As indicated in the figure, two way communication is allowed and there are independent random number generators at both the transmitter and the receiver. Two way communication is essential to distinguish the receiver from the eavesdropper. Having random number generators at both ends is not as basic a requirement, and is only needed in some implementations.

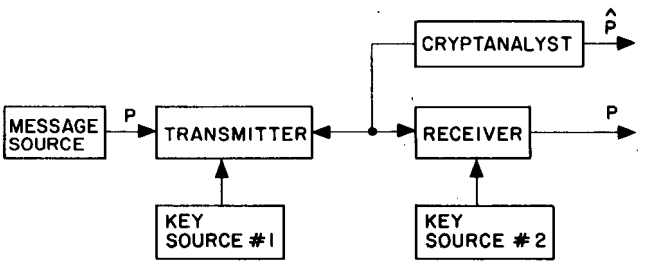


Fig. 2. Public Key Cryptographic System.

The situation is analogous to having a room full of people who have never met before and who are of equal mathematical ability. I choose one other person in the room and, with everyone else listening, give him instructions which allow the two of us to carry on a conversation that no one else can understand. I then choose another person and do the same with him.

This sounds somewhat impossible and, from one point of view, it is. If the cryptanalyst had unlimited computer time he could understand everything we said. But that is also true of most conventional cryptographic systems—the cryptanalyst can try all keys until he finds the one that yields a meaningful decipherment of the intercepted message. The real question is whether we can, with very limited computations, exchange a message which would take the cryptanalyst eons to understand using the most powerful computers envisionable.

A public key cryptosystem [4] has two keys, one for enciphering and one for deciphering. While the two keys effect inverse operations and are therefore related, there must be no easily computed method of deriving the deciphering key from the enciphering key. The enciphering key can then be made public without compromising the deci-

phering key so that anyone can encipher messages, but only the intended recipient can decipher messages.

The conventional cryptosystem of Fig. 1 can be likened to a mathematical strongbox with a resettable combination lock. The sender and receiver use a secure channel to agree on a combination (key) and can then easily lock and unlock (encipher and decipher) messages, but no one else can.

A public key cryptosystem can be likened to a mathematical strongbox with a new kind of resettable combination lock that has two combinations, one for locking and one for unlocking the lock. (The lock does not lock if merely closed.) By making the locking combination (enciphering key) public anyone can lock up information, but only the intended recipient who knows the unlocking combination (deciphering key) can unlock the box to recover the information.

Public key and related cryptosystems have been proposed by Merkle [5], Diffie and Hellman [4], Rivest *et al.* [6], Merkle and Hellman [7], and McEliece [8]. We will only outline the approaches, and the reader is referred to the original papers for details.

Electronic mail unlike ordinary mail is machine readable and can be automatically scanned for sensitive messages.

The RSA (Rivest *et al.*) scheme [6] is based on the fact that it is easy to generate two large primes and multiply them together, but it is much more difficult to factor the result. (Try factoring 518940557 by hand. Then try multiplying 15107 by 34351.) The product can therefore be made public as part of the enciphering key without compromising the factors which effectively constitute the deciphering key. By making each of the factors 100 digits long, the multiplication can be done in a fraction of a second, but factoring would require billions of years using the best known algorithm.

As with all public key cryptosystems there must be an easily implemented algorithm for choosing an enciphering-deciphering key pair, so that any user can generate a pair, regardless of his mathematical abilities. In the RSA scheme the key generation algorithm first selects two large prime numbers p and q and multiplies them to produce $n = pq$. Then Euler's function is computed as $\phi(n) = (p-1)(q-1)$. ($\phi(n)$ is the number of integers between 1 and n which have no common factor with n. Every p^{th} number has p as a common factor with n and every q^{th} number has q as a common factor with n.) Note that it is easy to compute $\phi(n)$ if the factorization of n is known, but computing $\phi(n)$ directly from n is equivalent in difficulty to factoring n [6].

$\phi(n)$ as given above has the interesting property that for any integer a between 0 and $n-1$ (the integers modulo n) and any integer k

$$a^{k\phi(n)+1} = a \mod n. \tag{1}$$

Therefore, while all other arithmetic is done modulo n, arithmetic in the exponent is done modulo $\phi(n)$.

A random number E is then chosen between 3 and $\phi(n) - 1$ and which has no common factors with $\phi(n)$. This then allows

$$D = E^{-1} \mod \phi(n) \tag{2}$$

to be calculated easily using an extended version of Euclid's algorithm for computing the greatest common divisor of two numbers [9, p. 315, problem 15; p. 523, solution to problem 15].

THE RIVEST–SHAMIR–ADLEMAN PUBLIC KEY SCHEME

Design

Find two large prime numbers p and q, each about 100 decimal digits long. Let $n = pq$ and $\psi = (p-1)(q-1)$.

Choose a random integer E between 3 and ψ which has no common factors with ψ. Then it is easy to find an integer D which is the "inverse" of E modulo ψ, that is, $D \cdot E$ differs from 1 by a multiple of ψ.

The public information consists of E and n. All other quantities here are kept secret.

Encryption

Given a plaintext message P which is an integer between 0 and $n-1$ and the public encryption number E, form the ciphertext integer

$$C = P^E \mod n.$$

In other words, raise P to the power E, divide the result by n, and let C be the remainder. (A practical way to do this computation is given in the text of Hellman's paper.)

Decryption

Using the secret decryption number D, find the plaintext P by

$$P = C^D \mod n.$$

Cryptanalysis

In order to determine the secret decryption key D, the cryptanalyst must factor the 200 or so digit number n. This task would take a million years with the best algorithm known today, assuming a 1 μs instruction time.

The information (E,n) is made public as the enciphering key and is used to transform unenciphered, plaintext messages into ciphertext messages as follows: a message is first represented as a sequence of integers each between 0 and $n-1$. Let P denote such an integer. Then the corresponding ciphertext integer is given by the relation

$$C = P^E \bmod n. \tag{3}$$

The information (D,n) is used as the deciphering key to recover the plaintext from the ciphertext via

$$P = C^D \bmod n. \tag{4}$$

These are inverse transformations because from (3), (2), and (1)

$$C^D = P^{ED} = P^{k\phi(n)+1} = P. \tag{5}$$

As shown by Rivest *et al.*, computing the secret deciphering key from the public enciphering key is equivalent in difficulty to factoring n.

As a small example suppose $p = 5$ and $q = 11$. Then $n = 55$ and $\phi(n) = 40$. If $E = 7$ then $D = 23$ ($7 \times 23 = 161 = 1 \bmod 40$). If $P = 2$, then

$$C = 2^7 \mod 55 = 18 \tag{6}$$

and

$$C^D = 18^{23} \mod 55 \tag{7}$$

$$= 18^1 18^2 18^4 18^{16} \tag{8}$$

$$= 18\ 49\ 36\ 26 \mod 55 \tag{9}$$

$$= 2 \tag{10}$$

which is the original plaintext.

Note that enciphering and deciphering each involve an exponentiation in modular arithmetic and that this can be accomplished with at most $2(\log_2 n)$ multiplications mod n. As indicated in (8), to evaluate $Y = a^X$, the exponent X is represented in binary form, the base a is raised to the 1st, 2nd, 4th, 8th, etc. powers (each step involving only one squaring or multiplication), and the appropriate set of these are multiplied together to form Y.

Merkle and Hellman's method [7] makes use of trap-door knapsack problems. The knapsack problem is a combinatorial problem in which one is given a vector of n integers, $\mathbf{a}$, and an integer S which is a sum of a subset of the $\{a_i\}$. The problem is to solve for the subset, or equivalently, for the binary vector $\mathbf{x}$ which is the solution to the equation

$$S = \mathbf{a} * \mathbf{x}. \tag{11}$$

While the knapsack problem is very difficult to solve in general, there are specific cases which are easy to solve. For example, if the knapsack vector is

$$\mathbf{a}' = (171, 197, 459, 1191, 2410) \tag{12}$$

then, given any S', $\mathbf{x}$ is easily found because each component of $\mathbf{a}'$ is larger than the sum of the preceding components. If $S' = 3798$, then it is seen that x_5 must be 1 because, if it were 0, $a_5' = 2410$ would not be in the sum and the remaining elements sum to less than S'. After subtracting the effect of a_5' from S', the solution continues recursively and establishes that $x_4 = 1$, $x_3 = 0$, $x_2 = 1$, and $x_1 = 0$.

The knapsack vector

$$\mathbf{a} = (5457, 4213, 5316, 6013, 7439) \tag{13}$$

does not possess the property that each element is larger than the sum of the preceding components, and the simple method of solution is not possible. Given $S = 17665$, there is no obvious method for finding that $\mathbf{x} = (0,1,0,1,1)$ other than trying almost all 2^5 subsets.

But it "just so happens" that if each component of $\mathbf{a}$ is multiplied by 3950 modulo 8443 the vector $\mathbf{a}'$ of (12) is obtained. By performing the same transformation on S, the quantity $S' = 3798$ is obtained. It is now seen that there is a simple method for solving for $\mathbf{x}$ in the equation

$$S = \mathbf{a} * \mathbf{x} \tag{14}$$

by transforming to the easily solved knapsack problem

$$S' = \mathbf{a}' * \mathbf{x}. \tag{15}$$

The two solutions $\mathbf{x}$ are the same provided the modulus is greater than the sum of the $\{a_i'\}$.

The variables of the transformation (the multiplier 3950 and the modulus 8443) are secret, trap-door information used in the construction of the trap-door knapsack vector $\mathbf{a}$. There is no apparent, easy way to solve knapsack problems involving $\mathbf{a}$ unless one knows the trap-door information.

When $\mathbf{a}$ is made public anyone can represent a message as a sequence of binary $\mathbf{x}$ vectors and transmit the information securely in the corresponding sums, $S = \mathbf{a} * \mathbf{x}$. The intended recipient uses his trap-door information (secret deciphering key) to easily solve for $\mathbf{x}$, but no one else can do this. Of course the $\mathbf{a}$ vector must be significantly longer than that used in this small, illustrative example.

McEliece's public key cryptosystem [8] is based on algebraic coding theory. Goppa codes are highly efficient error correcting codes [10], but their ease of error correction is destroyed if the bits which make up a codeword are scrambled prior to transmission. To generate a public enciphering key, a user first selects a Goppa code chosen at random from a large set of possible codes. He then selects a permutation of the codeword bits, computes the generator matrix associated with the scrambled Goppa code and makes it public as his enciphering key. His secret deciphering key is the permutation and choice of Goppa code.

Key distribution, the secure transmission of keys to the users who need them, is a major problem in securing a communication network.

Anyone can easily encode information (scrambling does not greatly increase the difficulty of encoding since the scrambled code is still linear), add a randomly generated error vector, and transmit this. But only the intended recipient knows the inverse permutation which allows the errors to be corrected easily.

McEliece estimates that a block length of 1000 bits with 500 information bits should foil cryptanalysis using the best currently known attacks.

The other two known methods for communicating securely over an insecure channel without securely transmitting a key are not true public key cryptosystems. Rather, they are public key distribution systems which are used to securely exchange a key over an insecure

channel without any prearrangement, and that key is then used in a conventional cryptosystem.

Merkle's technique [5] involves an exchange of "puzzles." The first user generates n potential keys and hides them as the solutions to n different puzzles, each of which costs n units to solve. The second user chooses one of the n puzzles at random, solves it, and sends a test message encrypted in the associated key. The first user determines which key was chosen by trying all n of them on the test message.

The cost to the first user is proportional to n. He must generate and store n keys, generate and transmit n puzzles, and try n keys on the test message. The cost to the second user is also proportional to n because he must solve one puzzle which was designed to have solution cost equal to n.

The cost to an eavesdropper appears to grow as n^2. He can try solving puzzles at random and see if the associated key (solution) agrees with the test message. On the average, he must solve $n/2$ puzzles, each at a cost of n.

Diffie and Hellman [4] describe a public key distribution system based on the discrete exponential and logarithm functions. If q is a prime number and a is a primitive element, then X and Y are in a 1:1 correspondence for $1 \leqslant X, Y \leqslant (q-1)$ where

$$Y = a^x \mod q \tag{16}$$

and

$$X = \log_a Y \quad \text{over } GF(q). \tag{17}$$

While the discrete exponential function (16) is easily evaluated, as in (7) and (8), no general, fast algorithms are known for evaluating the discrete logarithm function (17). Each user chooses a random element X and makes the associated Y public. When users i and j wish to establish a key for communicating privately they use

$$K_{ij} = a^{X_i X_j} \tag{18}$$

$$= (Y_i)^{X_j} = (Y_j)^{X_i}. \tag{19}$$

Equation (19) demonstrates how both users i and j use the easily computed discrete exponential function to calculate K_{ij} from their private and the other user's public information. An opponent who knows neither user's secret information can compute K_{ij} if he is willing to compute a discrete logarithm, but that can be made computationally infeasible using the best currently known algorithms [11].

The various public key systems are compared in Section V.

IV. DIGITAL SIGNATURES

Business runs on signatures and, until electronic communications can provide an equivalent of the written signature, it cannot fully replace the physical transportation of documents, letters, contracts, etc.

Current digital authenticators are letter or number sequences which are appended to the end of a message as a crude form of signature. By encrypting the message and authenticator with a conventional cryptographic system, the authenticator can be hidden from prying eyes. It therefore prevents third party forgeries. But, because the authentication information is *shared* by the sender and receiver, it cannot settle disputes as to what message, if any, was sent. The receiver can give the authentication information to a friend and ask him to send a signed message of the receiver's choosing. The legitimate sender of messages will of course deny having sent this message, but there is no way to tell whether the sender or receiver is lying. The whole concept of a contract is embedded in the possibility of such disputes, so stronger protection is needed.

A true digital signature must be a number (so it can be sent in electronic form) which is easily recognized by the receiver as validating the particular message received, but which could only have been generated by the sender. It may seem impossible for the receiver to be able to recognize a number which he cannot generate, but such is not the case.

While there are other ways to obtain digital signatures, the easiest to understand makes use of the public key cryptosystems discussed in the last section. The i^{th} user has a public key E_i and a secret key D_i. This notation was chosen because E_i was used to encipher and D_i was used to decipher. Suppose, as in the RSA scheme, the enciphering function is **onto**, that is, for every integer C less than n, there exists an integer m for which $E_i(m) = C$. Then, we can interchange the order of operations and use D_i first to sign the message and E_i second to validate the signature. When user i wants to sign and send a message M to user j, he operates on M with his secret key D_i to obtain

$$C = D_i(M) \tag{20}$$

which he then sends to user j. User j obtains i's public key E_i from a public file and operates with it on C to obtain M

$$E_i(C) = E_i[D_i(M)] = M \tag{21}$$

User j saves C as proof that message M was sent to him by user i. No one else could have generated C, because only i knows D_i. And if j tries to change even one bit in C, he changes its entire meaning (such error propagation is necessary in a good cryptosystem).

If i later disclaims having sent message M to user j, then j takes C to a "judge" who accesses the public file and checks whether $E_i(C)$ is a meaningful message with the appropriate date, time, address, name, etc. If it is, the judge rules in favor of j. If it is not, the ruling is in favor of i.

Digital signatures have an advantage over written signatures because written signatures look the same, independent of the message. My signature is supposed to look the same on a $100 check as on a $1000 check, so a dishonest recipient can try to alter the check. Similarly, if a photostat of a contract is acceptable as proof, a dishonest person can alter the contract and make a copy which hides the alteration. Such mischief is impossible with digital signatures, provided the signature system is truly secure.

The disadvantage of digital signatures is that the ability to sign is equivalent to possession of a secret key. This key will probably be stored on a magnetic card which, unlike the ability to sign one's name, can be stolen.

V. COMPARISON OF PUBLIC KEY SYSTEMS

This section compares the public key systems which have been proposed. Speed, ease of signature genera-

tion, and certain other characteristics can be compared more readily than the all important question of security level. We can compare the security level using the best known methods for breaking each system, but there is the danger that better methods will be found which will change the relative rankings.

If signatures are desired, attention should be directed primarily to the RSA [6] and trap-door knapsack systems [7]. The RSA scheme yields signatures directly. While the trap-door knapsack signature method described in [7] is not direct, Merkle and Reeds have developed a method for generating "high density" trap-door knapsacks which simplify signature generation, and Shamir has recently suggested a direct method for obtaining signatures. Both of these approaches are not yet published.

The $a^{(X_1,X_2)}$ and Goppa code methods do not appear to lend themselves to signatures, but Merkle has developed a puzzle-like technique for generating signatures.

So far, as storage requirements for the public file, the $a^{(X_1,X_2)}$ and RSA schemes are most interesting. Each requires on the order of 500 bits of storage per user. The trap-door knapsack scheme requires on the order of 100 kbits of storage per user, and the Goppa code method requires on the order of a megabit per user. Merkle's puzzle scheme is not really suited to public file storage and rather depends on transmission of public information at the start of each new conversation. The transmitted information must be on the order of a gigabit before significant levels of security are afforded.

Instead of storing each user's public key in a public file (similar to a telephone book), Kohnfelder [12] has suggested having the system give each user a signed message, or certificate, stating that user's public key. The certificate could be stored by the user on a magnetic card, and transmitted at the start of a conversation. This method converts public file storage requirements into transmission requirements. The system's public key would be needed to check the certificate and could be published widely. Protecting the system's secret key might be easy because no one else ever has to use it and it could be destroyed after it was used to certify a group of users.

Computation time on the part of the legitimate users is smallest with the trap-door knapsack method. The $a^{(X_1X_2)}$ and RSA schemes each require several hundred times as much computation, but are still within reason. Merkle's technique requires even more computation. The Goppa code technique is extremely fast for enciphering, requiring approximately 500 XOR's on 1000 bit vectors, but I have not yet estimated its deciphering requirements.

Turning to security level, Merkle's puzzle method [5] has the advantage of being the most solid method for communicating securely over an insecure channel. That is, it is extremely doubtful that a better method will be found for breaking it. Unfortunately, it is also the least secure using the best known algorithm. Its work factor (ratio of cryptanalytic effort to enciphering and deciphering effort, using the best known algorithms) is only n^2:n. Since encryption should cost on the order of \$0.01 and cryptanalysis should cost on the order of \$10 million or more, this ratio needs to be 10^9 or more and corresponds to $n = 10^9$. If all of the enciphering and deciphering effort were in computation, this might be possible in the near future (a \$10 microprocessor can execute on the order of 1 million instructions per second), but Merkle's method requires n transmissions as well as n operations on the part of the legitimate users. Current technology therefore limits Merkle's scheme to $n \leqslant 10\,000$ which corresponds to approximately 500 kbits of transmission. If fiber optic or other low cost, ultra-high bandwidth communication links become available, Merkle's technique would become of greater practical interest.

Diffie and Hellman's exponentiation method [4] requires the legitimate users to perform an exponentiation in modular arithmetic while the best known cryptanalytic method requires the computation of a logarithm in modular arithmetic. Exponentiation is easily accomplished in at most $2b$ multiplications, much as in (8), where b is the number of bits in the representation of the modulus. Each multiplication can be accomplished with at most $2b$ additions or subtractions, and each of these operations involves at most b gate delays for the propagation of carry signals. Overall, an exponentiation in modular arithmetic can be accomplished in at most $4b^3$ gate delays.

Computation of a logarithm in modular arithmetic is much more complex, and the best currently known algorithm [11] requires $2^{b/2}$ or more operations provided the modulus is properly chosen. Each operation involves a multiplication, or $2b^2$ gate delays. The work factor is therefore exponential in b.

If $b = 500$, then 500 million gate delays are required at the legitimate users' terminals. With current technology this can be accomplished in several seconds, a not unreasonable delay for establishing a key during initial connection. Using $b = 500$ results in the cryptanalyst having to do more than 10^{75} times as much work as the legitimate users, a very safe margin. The real question is whether better methods exist for computing logarithms in modular arithmetic, or if it is even necessary to compute such a logarithm to break this system.

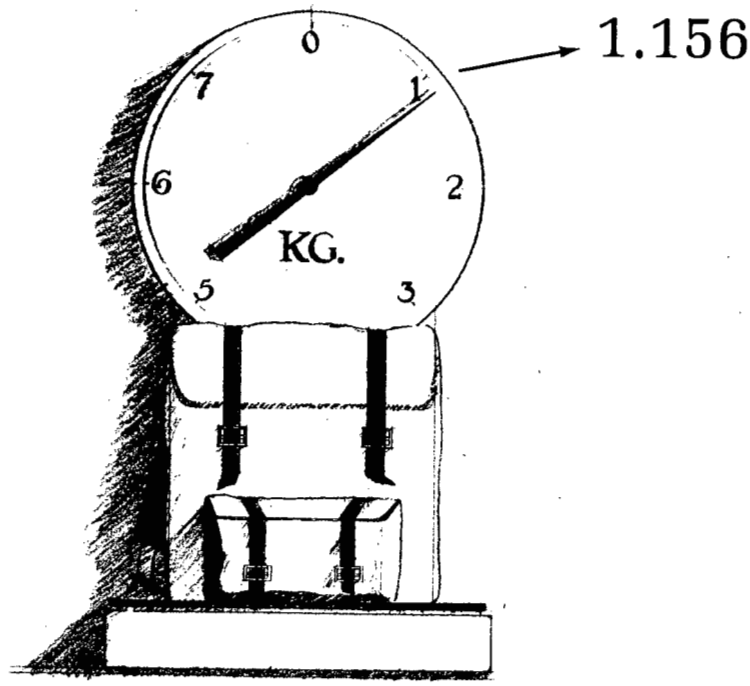
The following table gives the number of operations and time required for cryptanalysis for various values of b assuming a 1 μs instruction time:

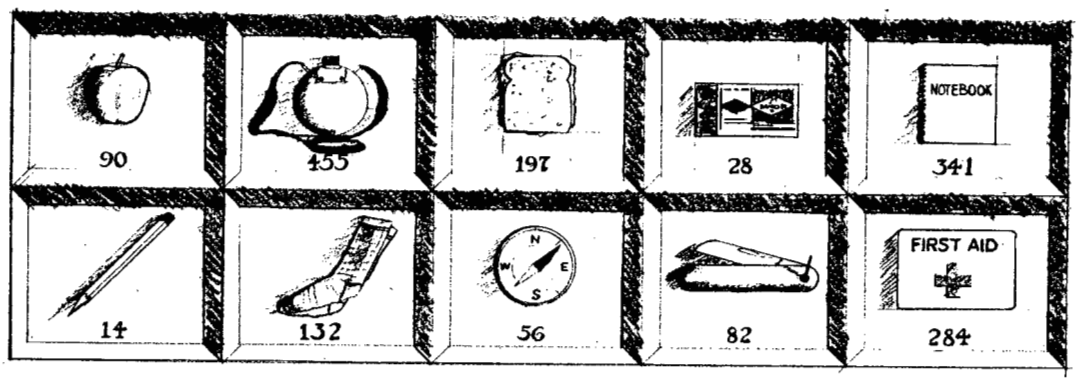
b (bits)	100	200	300	500	750	1000
Operations	1.1×10^{15}	1.3×10^{30}	1.4×10^{45}	1.8×10^{75}	7.7×10^{112}	3.3×10^{150}
Time (yrs.)	36	4×10^{16}	5×10^{31}	6×10^{61}	2×10^{99}	1×10^{137}

The storage requirements of this system are small. The public file stores a single b-bit number for each user and only several b-bit words of memory are required at the transmitter and receiver, so that single chip implementation is possible for b on the order of 500.

The RSA system [6] also requires that the legitimate users perform a modular exponentiation, but cryptanalysis is equivalent to factoring a b-bit number. Schroeppel has developed a new, as yet unpublished factoring algorithm which appears to require approximately $\exp\{[\ln(n)\ \ln(\ln n)]^{1/2}\}$ machine cycles where $n = 2^b$ is the number to be factored. The following

THE KNAPSACK PROBLEM





The knapsack is filled with a subset of the items shown, with weights indicated in grams. Given the weight of the filled knapsack, 1156 grams, can you determine which of the items are contained in the knapsack? (The scale is calibrated to deduct the weight of the empty knapsack.)

This simple version of the classic knapsack problem generally becomes computationally infeasible when there are 100 items rather than 10 as in this example. However, if the set of weights for the items happens to have some nice properties known only to someone with special "trap-door" information, then that person can quickly decipher the secret information, i.e., a 100 bit binary word that specifies which of the items are in the knapsack.

ART: Jeff Wyszkowski

table gives the number of operations and time to factor a b-bit number again assuming a 1 μs instruction time:

b (bits)	100	200	300	500	750	1000
Operations	2.8×10^{7}	2.3×10^{11}	2.9×10^{14}	3.6×10^{19}	5.8×10^{24}	1.8×10^{29}
Time	30 s	3 days	9 yr	1 Myr	2 Gyr	6×10^{15} yr

Public file storage for the RSA scheme is reasonable, being several hundred to a thousand bits per user. Memory requirements at the transmitter and receiver are also comparable to the $a^{(X_1X_2)}$ scheme, so that a single chip device can be built for enciphering and deciphering.

The best known method of cryptanalyzing the trap-door knapsack system requires on the order of $2^{n/2}$ operations where n is the size of the knapsack vector. Enciphering requires at most n additions, so the work factor is exponential. If n is replaced by b, the first table above gives the cryptanalytic effort required for various values of n, so $n \geqslant 200$ provides relatively high security levels. Since each element of the $\boldsymbol{a}$ vector is approximately $2n$ bits long, if $n = 200$, the public storage is approximately 80 kbits/user. Memory requirements at the transmitter and receiver are on the same order.

Both enciphering and deciphering require less computation than either the $a^{(X_1X_2)}$ or RSA scheme. Enciphering requires at most n additions and deciphering requires one multiplication in modular arithmetic, followed by at most n subtractions.

Until electronic communications can provide an equivalent of the written signature, it cannot fully replace the physical transportation of documents, letters, contracts, etc.

Care must be exercised in interpreting these tables. First, they assume that the cryptanalyst uses the best currently known method, and there may be much faster approaches. For example, prior to the development of Schroeppel's algorithm, the best factoring algorithm appeared to require $\exp\{[2\ \ln(n)\ \ln(\ln n)]^{1/2}\}$ operations. When $b = 200$, that would have predicted that 360 yr, not 3 days, would be required for cryptanalysis. There is the danger that even faster algorithms will be found, necessitating a safety margin in our estimates. As demonstrated by this example, the safety margin is needed in the exponent, not the mantissa.

A similar comment applies to the seemingly higher security level afforded by the $a_i^{(X_1X_2)}$ and trap-door knapsack methods when compared to the RSA scheme. For a given value of b the two tables show that the RSA scheme requires much less computation to break, using the best currently known techniques. But it is not clear whether this is because factoring is inherently easier than computing discrete logarithms or solving knapsack problems, or whether it is due to the greater study which has been devoted to factoring.

As computers become faster and more parallel, the time for cryptanalysis also falls. A 1 ns computer with million-fold parallelism might reduce the time estimates given in the tables by a factor of 10^9.

VI. CONCLUSIONS

We are in the midst of a communications revolution which will impact many aspects of people's every day lives. Cryptography is an essential ingredient in this revolution, and is necessary to preserve privacy from computerized censors capable of scanning millions of pages of documents for even one sensitive datum. The public key and digital signature concepts are necessary in commercial systems because of the large number of interconnections which are possible, and because of the need to settle disputes.

A major problem which confronts cryptography is the certification of these systems. How can we decide which proposed systems really are secure, and which only appear to be secure? Proofs are not possible using the currently developed theory of computational complexity and, while such proofs may be possible in the future, something must be done immediately. The currently accepted technique for certifying a cryptographic system as secure is to subject it to a mock attack under circumstances which are extremely favorable to the cryptanalyst and unfavorable to the system. If the system resists such a concerted attack under unfavorable conditions, it is hoped that it will also resist attacks by one's opponents under more realistic conditions.

Governments have built up expertise in the certification area but, due to security constraints, this is not currently available for certification of commercially oriented systems. Rather, this expertise in the hands of a foreign government poses a distinct threat to a nation's businesses. It has even been suggested that poor or nonexistent encryption will lead to international economic warfare, a concern of importance to national security. (There is speculation that this occurred with the large Russian grain purchases of several years ago.)

There is a tradeoff between this and other national security considerations which needs to be resolved, but the handling of the national data encryption standard indicates that public discussion and resolution of the tradeoff is unlikely unless individuals make their concern known at a technical and political level.

REFERENCES

[1] W. Diffie and M. E. Hellman, "Exhaustive cryptanalysis of the NBS data encryption standard," *Computer*, pp. 74–84, June 1977.

[2] D. Branstad, "Encryption protection in computer data communications," presented at the IEEE Fourth Data Communications Symposium, Oct. 7–9, 1975, Quebec, Canada.

[3] *IBM Syst. J., (Special Issue on Cryptography)*, vol. 17, no. 2, 1978.

[4] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 644–654, Nov. 1976.

[5] R. C. Merkle, "Secure communication over an insecure channel," *Common. Ass. Comput. Mach.*, vol. 21, pp. 294–299, Apr. 1978.

[6] R. L. Rivest, A. Shamir, and L. Adleman, "On digital signatures and public key cryptosystems," *Commun. Ass. Comput. Mach.*, vol. 21, pp. 120–126, Feb. 1978.

[7] R. C. Merkle and M. E. Hellman, "Hiding information and signatures in trap-door knapsacks," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 525–530, Sept. 1978.

[8] R. J. McEliece, "A public key system based on algebraic coding theory," JPL DSN Progress Rep., 1978.
[9] D. E. Knuth, *The Art of Computer Programming, Vol. 2, Seminumerical Algorithms*. Reading, MA: Addison-Wesley, 1969.
[10] E. R. Berlekamp, "Goppa codes," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 590–592, Sept. 1973.
[11] S. C. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance, *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 106–110, Jan. 1978.
[12] L. Kohnfelder, *Towards a Practical Public-Key Cryptosystem*, M.I.T. Lab. for Comput. Sci., June 1978.

Martin E. Hellman (S'63–M'69) was born in New York, NY, on October 2, 1945. He received the B.E. degree in electrical engineering from New York University, New York, NY, in 1966, and the M.S. and Ph.D. degrees in electrical engineering from Stanford University, Stanford, CA, in 1967 and 1969, respectively.

During 1968 to 1969 he was at the IBM Thomas J. Watson Research Center. From 1969 to 1971 he was an Assistant Professor of Electrical Engineering at M.I.T. He is currently an Associate Professor of Electrical Engineering at Stanford University, doing research in the areas of cryptography and information theory.

Dr. Hellman is a member of Tau Beta Pi, Eta Kappa Nu and Sigma Xi, and consults in the areas of communications and information theory. He is a past president of the San Francisco Section's Information Theory Chapter and is a member of the Information Theory Group's Board of Governors.

Some General Interest Books on Cryptology

Selected by A. M. Bush, Book Reviews Editor

The field of cryptology has long been of interest, particularly in the affairs of governments. Because of its sensitive nature, the field exists in the shadows of the public domain, rather than in the forefront of current publicity. The following list of books, mostly of general interest and of more historical than current perspective may be useful to those who hold an interest in the field. The list should not be assumed to be exhaustive or complete.

Paul W. Blackstock, *The Secret Road to World War II: Soviet Versus Western Intelligence 1921–1939*. New York: Quadrangle Books, 1969.

Burke Davis, *Get Yamamoto*. New York: Random House, 1969.

Allen W. Dulles, *The Secret Surrender*. New York, Evanston, London: Harper and Row, 1966.

Ladislas Farago, *The Broken Seal*. New York: Random House, 1967.

Alexander Foote, *Handbook for Spies*. New York: Doubleday, 1979.

William F. and Elizabeth S. Friedman, *The Shakespearean Cipher Examined*. New York: Cambridge University Press, 1957.

Helen F. Gaines, *Cryptanalysis*. New York: Dover, 1956.

Joseph S. Galland, *An Historical and Analytical Bibliography of the Literature of Cryptology*. New York: AMS Press, 1945.

A. A. Hoebling, *The Week Before Pearl Harbor*. New York: Norton, 1963.

Admiral Sir William James, *The Code Breakers of Room 40*. New York: St. Martin's, 1956.

David Kahn, *The Codebreakers*. New York: Macmillan, 1967.

Husband E. Kimmel, *Admiral Kimmel's Story*. Chicago: Regnery, 1955.

Abraham L. Lavine, *Circuits of Victory*. Garden City, NY: Doubleday and Page, 1921.

Walter Lord, *Incredible Victory*. New York, Evanston, London: Harper and Row, 1967.

J. C. Masterman, *The Double-Cross System in the War of 1939–1945*. New Haven and London: Yale University Press, 1972.

Donald McLachlan, *Room 39: A Study in Naval Intelligence*. New York: Atheneum, 1968.

Dan T. Moore and Martha Waller, *Cloak and Cipher*. New York and Indianapolis: Bobbs–Merrill.

George Morgenstern, *Pearl Harbor: The Story of the Secret War*. New York: Devin-Adair, 1947.

Gilles Perrault, *The Secret of D-Day*. Translated from the French by Len Ortzen. Boston, Toronto: Little, Brown, 1964.

Fletcher Pratt, *Secret and Urgent*. Garden City, NY: Blue Ribbon Books, 1942.

Abraham Sinkov, *Elementary Cryptanalysis: A Mathematical Approach*. New York: Random House, 1970.

Laurence D. Smith, *Cryptography*. New York: Norton, 1943.

Sir Kenneth Strong, *Men of Intelligence*. New York: St. Martin's, 1972.

Robert A. Theobald, Rear Admiral, U.S.N., (Ret.) *The Final Secret of Pearl Harbor*. New York: Devin-Adair, 1954.

Hans L. Trefousse, Ed., *What Happened at Pearl Harbor*. New York: Twayne Publishers, 1958.

Barbara Tuchman, *The Zimmermann Telegram*. New York: Viking, 1958.

Roberta Wohlstetter, *Pearl Harbor: Warning and Decision*. Stanford: Stanford University Press, 1962.

James R. Wolfe, *Secret Writing*. New York: McGraw-Hill, 1970.

Herbert O. Yardley, *The American Black Chamber*. Indianapolis: Bobbs–Merrill, 1931.

Ellis M. Zacharias, *Secret Missions: The Story of an Intelligence Officer*. New York: Putnam, 1946.