The Use of Public Key Cryptography in Communication System Design

Leonard M. Adleman AND Ronald L. Rivest

A public key cryptosystem can be synergistically combined with a traditional system to obtain the best features of both approaches.

Abstract—**Since the time of Caesar, cryptography has been used in the design of secure communications systems. Recently, Diffie and Hellman [2] have introduced a new type of cryptographic method, based on "trapdoor" functions, which promises to be of great value in the design of such systems. We present a review of public key cryptosystems, followed by examples of communications systems which make particularly elegant use of their properties.**

I. A REVIEW OF PUBLIC KEY CRYPTOSYSTEMS

Public key cryptosystems were introduced by Diffie and Hellman in [2] where the interested reader will find a complete, easily readable exposition. The reader already familiar with such systems may prefer to skip to the examples in Section III.

In a traditional (nonpublic key) cryptosystem there is a general encryption procedure E into which a key K and a message M may be put in order to produce a cipher text C: formally $E(K,M) = C$. There is also a general decryption procedure D into which a key K and a cipher text C may be put in order to produce a message M: $D(K,C) = M$. Any such system has the following properties.

1) Decryption reverses encryption:

$$D(K,E(K,M)) = M.$$

2) It is "impractical" to decrypt without the appropriate key.

In a traditional system, if party A wishes to communicate with party B over a tapped line, the following steps are taken:

1) A and B communicate a key K which is unknown to all others (this may be accomplished via secure courier for example).

2) A encrypts his message M using E and K and sends the resulting ciphertext $C = E(M,K)$ to B.

3) B uses D and K to regain the message $M = D(K,C)$.

Clearly, to maintain the security of such a system, the key K must be kept secret.

A public key cryptosystem differs only slightly in overall plan from a traditional system. There is a general

For a more extensive discussion of the various public key cryptosystems, see the paper by Hellman in this issue.

The research of L. M. Adleman was sponsored in part by NSF Grant MCS78-04343 and in part by the Office of Naval Research Grant N00014-67-0204-0063. The research of R. L. Rivest was sponsored in part by NSF Grant MCS76-14294. This paper was prepared for presentation at the National Telecommunications Conference (NTC'78), Birmingham, AL, December 4–6, 1978, and will appear in the *NTC'78 Conference Record*.

L. M. Adleman is with the Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139.

R. L. Rivest is with the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139.

0148-9615/78/1100-0020$00.75 ©1978 IEEE

encryption procedure E into which a key K and a message M may be put to produce a cipher text $C = E(K,M)$. There is also a general decryption procedure D which takes cipher text and keys and produces messages. However, unlike the traditional system in which the same key is used to encrypt and decrypt, in a public key system each key K used to encrypt has a mate $K' \neq K$ which is used to decrypt. From now on we will denote the key used to encrypt by K_E and the one used to decrypt by K_D. As with a traditional system we want the following properties:

a) Decryption reverses encryption:

$$D(K_D,E(K_E,M)) = M.$$

b) It is "impractical" to decrypt without the appropriate key. (In particular K_E cannot be used to decrypt:

$$D(K_E,E(K_E,M)) \neq M.)$$

In addition, we will require the following properties:

c) It is practical (easy on a computer) to generate mated pairs $<K_E,K_D>$.

d) It is "impractical" to obtain K_D from K_E.

It is property d) which is the source of a public key cryptosystem's somewhat paradoxical properties.

If A wishes to communicate with B over a tapped line using a public key cryptosystem, the following steps are taken:

1) B generates an encryption keyK_E and its decryption key mate K_D. K_D is kept by B and remains unknown to all others including A.

2) B sends K_E to A (the tapped line will suffice here since K_E need not be kept secret).

3) A encrypts his message M using E and K_E and sends the resulting ciphertext $C = E(K_E,M)$ to B.

4) B uses K_D and D to decrypt C and obtain $M = D(K_D,C)$.

Notice that the security of this system does not depend on keeping K_E secret. Even if K_E is publicly revealed, the security of the system is not endangered, since we have demanded that decrypting with K_E will not work $(D(K_E,E(K_E,M) = M)$, and it is "impractical" to obtain K_D from K_E. It is for this reason that the term "public key" is used.

For subtler applications (e.g., signatures [2],[6]) public key cryptosystems with additional properties are needed. In particular

e) Encryption reverses decryption

$$E(K_E,D(K_D,M)) = M.$$

f) It is "impractical" to encrypt without the appropriate key. (In particular K_D cannot be used to encrypt: $D(K_D,E(K_D,M)) \neq M.$)

g) It is "impractical" to obtain K_E from K_D.

For obvious reasons we will call a system with properties a)–g) a "double public key cryptosystem".

II. AN EXAMPLE OF A DOUBLE PUBLIC KEY CRYPTOSYSTEM

Several public key cryptosystems have been proposed in response to the Diffie–Hellman paper [5],[6]. Below we present an outline of the double system due to Rivest *et al.* [6]. The interested reader is encouraged to see [6] since important details are omitted here in order to facilitate the exposition.

1) To establish a mated pair K_E and K_D, the user first produces three large prime numbers p, q, and e. He next computes a number d such that $d \cdot e$ has a remainder of 1 when divided by $(p-1)\cdot(q-1)$ (i.e., $de = 1$ MOD $((p-1)(q-1))$). K_E is the pair of numbers $<e,n>$ and K_D is the pair of numbers $<d,n>$ where $n = p \cdot q$. (It is important that n be the result of multiplying p times q and not p and q themselves.)

2) The encryption procedure E takes a message M (thought of as a binary number, say in ASCII) and an encryption key $K_E = <e,n>$ and produces the cipher text C by raising M to the e^{th} power and taking the remainder when divided by n ($C = M^e$ MOD (n)).

3) The decryption procedure D takes a cipher text C and a decoding key $K_D = <d,n>$ and decrypts by raising C to the d^{th} power and taking the remainder when divided by n ($M = C^d$ MOD (n)).

Fast methods of finding large primes p, q, and e, of computing the appropriate d from them, and of encrypting and decrypting are given in [6]. Also see [6] for examples and arguments concerning the security of this double public key system.

III. EXAMPLES OF THE USE OF PUBLIC KEY CRYPTOSYSTEMS

A. Read Only Communications

This application comes from an article by Gina Bara Kolata which appeared recently in *Science*[1] [4].

As part of the Nuclear Test Band Treaty it has been suggested that seismographic devices be buried in Russian soil to monitor earth tremors and thereby detect nuclear activity (no doubt Russian devices would be placed in the U.S. as well). Apparently, the technology exists for implanting the devices and making them tamperproof; however, there is a concern over the security of the transmissions from them. Some method of protecting the transmissions from unauthorized insertion and deletion is necessary lest false transmissions indicating a halcyon state be sent while in fact testing is taking place. The obvious answer is for the U.S. to encrypt the transmissions thereby inhibiting tampering. Unfortunately, this creates a new problem since Russia has no assurance that only seismic information and not "spy" data is being transmitted. Simple monitoring will not help since the Russians cannot read the encrypted transmissions. In one proposed solution, based on traditional cryptography, Russia would record the encrypted transmissions, then at the end of each month the United States would surrender the encoding key used that month, enabling Russia to confirm in retrospect that only legitimate information was sent. Apparently, in these circles a month lag time is unsatisfactory, and any attempt to make the key exchange more frequent creates unacceptable key management risks.

[1] The scheme described may be due to Gus Simmons of Sandia.

The solution to the problem makes use of the special properties of a double public key cryptosystem. In this solution, the United States generates a mated pair of keys K_E and K_D. K_D is revealed to Russia (so in this system K_D is the "public key") while K_E is secured inside the seismographic device. All transmissions are encoded using K_E. Since both the U.S. and Russia have the decoding key K_D, each can monitor and decode the resulting outputs. However, Russia has not been given the private encoding key K_E, cannot obtain it from K_D, and therefore is unable to tamper with the transmissions. Thus, Russia has the facility to read the encrypted language, but not to write it, and apparently all design constraints have been satisfied.

Extremely high encryption rates without the problems of key distribution can be achieved by combining traditional systems with public key cryptosystems.

B. Securing Automatic Teller Machines

This system was designed by researchers at Interbank.

Automatic teller machines are in widespread use in this country. Twenty-four hours a day a user can approach a machine (usually located on the external wall of a bank) and using a protocol typically involving passwords and magnetic cards cause the device to deliver cash. Usually the ATM is connected via telephone lines to a central computer which does bookkeeping, and, when appropriate conditions are met, transmits commands for the release of money from the ATM. While there are issues of security concerning the use of passwords and magnetic cards, these will not concern us. We are interested in securing the line between the ATM and the central computer against insertion of messages which will cause illegitimate release of cash from the ATM. A traditional system of encryption along the lines works well here. Each ATM shares a key with the central computer, and this is used to encrypt along the line, thus inhibiting insertions. Unfortunately, this solution has associated key distribution problems. How is the key brought to the ATM? Transmission in the clear over telephone lines is obviously unacceptable. Delivery by couriers invites bribery and theft. Hard wiring of the key at the time the ATM is built creates security problems in the manufacturing environment, and does not allow for key changes.

The solution proposed by the researchers at Interbank makes elegant use of public key techniques. The central computer generates a mated pair of keys K_E and K_D. K_D is kept by the central computer and security measures must be taken to keep it secret. Each ATM is provided with the corresponding public key K_E. Since the security of the system will not depend on keeping K_E secret, there is no serious problem in distributing it to the ATM's. At the onset of a commercial transaction, the ATM generates a random number R to be used for this transaction only.[2] The ATM stores R, encrypts the message "This is ATM x the current transaction number is R" using K_E, and sends the resulting ciphertext to the central computer. The computer decrypts the ciphertext using K_D and stores R. R is then used as a key in a traditional (or public key) cryptosystem for encrypting and decrypting all communications between the computer and the ATM until a new transaction begins, at which time the ATM independently generates a new R and the process begins anew.

Two rules govern the use of the keys

a) The central computer ignores all messages it receives which are encrypted using K_E except those of the form "This is ATM ____ the current transaction number is ____" (we are not assuming the computer can distinguish messages (even in the correct form) which come from real ATM's and those which come from intruders).

b) The ATM ignores all messages it receives except those encrypted under the current R.

Surprisingly the key distribution problems have been solved. Even if the encryption key K_E is publicly revealed, it is of no value in defeating the system. If a prospective thief knows K_E, how could he cause money to be issued by the ATM? He does not know the current R since it has only appeared on the line encrypted using K_E and he does not know the decryption key K_D. By rule a) he can use K_E in just one way, to send the computer an encrypted message "This is ATM x the current transaction number is R'" for some R' of his choice. This will cause the computer to begin communicating with the ATM using R' instead of R, but by rule b), the ATM will steadfastly ignore all messages encrypted under R' and will therefore not release money.

This example illustrates how public key and traditional systems can be synergistically combined. A traditional system may possess valuable properties (for example, extremely high encryption rates) unavailable in public key systems, but the traditional system may also have associated problems (for example, key distribution) which can be solved using public key methods.

C. Distribution of Session Keys

A recent report by the MITRE Corporation [7] has dramatized the insecurity of telephone communications by revealing the ease with which microwave transmissions can be monitored. Apparently, for approximately $55 000 ($35 per line) an entire microwave link can be tapped (the ability to insert or delete messages in an undetectable manner is probably vastly more expensive). In response to this threat, several systems using traditional encryption have been developed [1],[3]. Typically, these systems involve the use of a hierarchy of keys: A "master key" which remains fixed for long periods (months or years) and "session keys" which are used for shorter periods (hours or days). A typical system for link encryption would involve the following steps:

1) A single master key is securely distributed to each node in the system (alternatively a different master key can be used for each pair of nodes).

2) When a session begins, say once a day, session keys are randomly generated and distributed to the nodes under encryption with the master key. This process is

[2] There are technical problems involved in generating random numbers which must be considered in the implementation of such a system.

complete when each pair of communicating nodes shares a unique key.

3) Messages are sent node to node, encrypted under the current session key shared by those nodes.

4) At the end of the session all session keys are destroyed.

The main advantages of these systems are

1) The master key is rarely used and when used only random numbers are encrypted. This reduces the key's vulnerability to cryptanalytic attack.

2) The session keys are used only for one day and if lost do not compromise communications on other days.

The main disadvantages of these systems are

1) The master key must be distributed securely.

2) The master key requires long-term protection and its loss compromises all session keys and in turn all communications.

With a public key approach these disadvantages can be minimized. For example,

1) At the beginning of each sesson, selected nodes generate mated pairs of keys $<K_E, K_D>$.

2) Each selected node sends (over insecure line) K_E to its neighbors.

3) Each neighbor responds by randomly generating a "session key" and sending it to the selected node encrypted under K_E. The selected node decrypts it using K_D. Again the process is complete when each pair of communicating nodes shares a unique key.

4) All K_D and K_E are destroyed.

5) Messages are sent node to node encrypted under the current session key.

6) At the end of the session all session keys are destroyed.

In this system there are no long-term keys. No key, public or traditional, is kept for longer than the length of a session. Thus we have the advantages of session keys without the disadvantages of long-term master keys.

REFERENCES

[1] F. Heinrich, "The network security center: A system network approach to computer network security," NBS Special Pub. 500-21-Vol 2.

[2] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, Nov. 1976.

[3] W. F. Ehrsam *et al.*, "A cryptographic key management scheme for implementing the data encryption standard [DES]," *IBM Sys. J.* vol. 17, no. 2, 1978.

[4] G. B. Kolata, "Cryptology: A secret meeting at IDA," *Science*, Apr. 14, 1978.

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

[6] R. Rivest *et al.*, "A method for obtaining digital signatures and public key cryptosystems," *Commun. ACM*, Feb. 1978.

[7] C. W. Sanders *et al.*, "Selected examples of possible approaches to electronic communication interception operations," *MITRE Tech. Rep. MTR-7461*, Jan. 1977.

Leonard Adleman received his Ph.D. degree at the University of California, Berkeley, in the Department of Electrical Engineering and Computer Science in 1976. He is currently assistant Professor of Mathematics at MIT, Cambridge, where he is also a member of the Laboratory for Computer Science. His area of specialization has been computational complexity with particular emphasis on number theoretic problems. More recently his interests have included public key cryptosystems and both theoretical and applied aspects of cryptography.

Ronald L. Rivest is currently Associate Professor of Computer Science at MIT, Cambridge, where he has been for five years. He obtained his Ph.D. in 1974 from Stanford University, California. His work has been primarily in the area of computational complexity and cryptography.

WITH THIS NEW INFO WE CAN INCREASE OUR PRODUCTIVITY AND INCREASE OUR SHARE OF THE MARKET. MODEST GROWTH STRATEGIES, HA! WAIT TIL THEY SEE THIS.
YOU WORKED HARD, STEVE, BUT YOU DISREGARDED COMPANY POLICY...
FORTE INDUSTRIE
... YOU USED UNSECURED COMMUNICATIONS. WHAT IF YOU WERE BEING OVERHEARD?
YOU KNOW, THIS COULD EVEN MEAN AN EXECUTIVE V.P. JOB FOR ME...
BUT...
GOOD WORK, ROCKO. THIS NEW DATA FROM FORTE INDUSTRIES IS JUST WHAT WE NEED TO INCREASE OUR CAPITAL EXPENDITURES AND REDUCE OUR PRESENT RESEARCH AND DEVELOPMENT!

ART: Jeff Wyszkowski