

Introduction to Public Key Cryptology

Classical Cryptology

Until 1976, cryptology was classical cryptology. Typical of cryptology were the substitution ciphers, the transposition ciphers, and the machines ciphers (like enigma) that we have studied so far. Classical cryptology is symmetric key cryptology – both parties to a communication use the same key. Either the same key is used for encryption and decryption or the decryption key can easily be determined from the encryption key.

Classical cryptology was “ruled” by Auguste Kerckhoffs’ (1835 – 1903) principles, which were stated in 1883. Kerckhoffs enumerated six principles for field ciphers.

Desiderata for military cryptography

It is necessary to distinguish between a system of enciphered writing designed for a temporary exchange of letters among several isolated persons, and a method of cryptography intended to control for an unlimited time the communications of different military leaders. The latter, indeed, may not change their conventions at will or at any given moment. Further, they should never keep on their persons any object or note that would be such as to shed light for the enemy on the meaning of any secret messages that might fall into his hands.

A large number of ingenious arrangements achieve the result desired in the first case. For the second a system must satisfy certain exceptional conditions which I will summarize under the following six headings:

1. The system must be practically, if not mathematically, indecipherable.
2. It must not rely upon secrecy, and it must be able to fall into the enemy's hands without disadvantage.

3. The key should be able to be communicated and stored without the help of written notes, and to be changed or modified at the will of the correspondents.
4. It must be usable for telegraphic communications.
5. It must be portable, and its handling and operation must not require the assistance of many people.
6. Finally, it is necessary, in light of the circumstances in which it must be used, that the system be easy to use, not requiring extreme mental effort nor the knowledge of a large number of rules that must be followed.

These principles appear in Kerckhoffs' 64-page *La Cryptographie militaire* (1883).

Only a few books in the history of science may be called great. Some of these report a technical innovation that radically alters the content of the science. Through the 19th century, Alberti's and Kasiski's were the two books of this kind in cryptology. Such books look inward.

Other great books look outward. They bring the science up to date – make it consonant with its time – and so renew its utility to men. They do this by assimilating developments in relevant fields ... , by summing up the lessons of recent experience and deducing their meaning for the current age, and by reorganizing the concepts of the science according to this new knowledge. This does not mean simple popularization, though such a work usually does have an organic persuasiveness. Rather, it amounts to a reorientation, a new perspective.

For 300 years, the only great book of this kind in cryptology was Porta's. He was the first to delineate a coherent image of cryptology. His ideas remained viable so long because cryptology underwent no essential change; communication was by messenger, and consequently the nomenclator reigned. But his views no longer sufficed after the invention of the telegraph. New conditions demanded new theses, new insights. And in 1883 cryptology got them in the form of its

second great book of the outward-looking kind, *La Cryptographie militaire*.

[Kerckhoffs' principles] still compromise the ideal which military ciphers aim at. ...

There appears to be a certain incompatibility among [the principles] that makes it impossible to institute all of them at once. The requirement that is usually sacrificed is the first. Kerckhoffs argues strongly against the notion of a field cipher that would simply resist solution long enough for the orders to be carried out. This is not enough, he said, declaring that "the secret matter in communications sent over a distance very often retains its importance beyond the day on which it was transmitted."

Perhaps the most startling requirement, at first glance, was the second. Kerckhoffs explained that by "system" he meant "the material part of the system; tableaux, code books, or whatever mechanical apparatus may be necessary," and not "the key proper." Kerckhoffs here makes for the first time the distinction, now basic to cryptology, between the general system and the specific key.

... Kerckhoffs second requirement has become widely accepted under a form that is sometimes called the fundamental assumption of military cryptography: that the enemy knows the general system. But he must still be unable to solve messages in it without knowing the secret key. *The Codebreakers* by David Kahn

The second requirement is often called Kerckhoff's law. This requirement means that a cryptosystem should be secure even if an enemy knows everything about the system except the key; it argues against "security through obscurity" – that the security of a cryptosystem would depend on keeping the method of encryption secret. The same idea was stated (in the 1940s) by Claude Shannon (1916 – 2001), the founder of information theory, as "the enemy knows the system." The latter is called Shannon's maxim.

Diffie-Hellman

What caused the changes that began in 1976 was the publication of the paper “New Directions in Cryptography” by Whitfield Diffie (b. 1944) and Martin Hellman (b. 1946). (*IEEE Transactions on Information Theory*, vol. 22, no. 6, November 1976).

Diffie and Hellman anticipated the needs of what has become the internet. They anticipated that there would be world-wide communication between people who had never met, and they posed the question: How would keys be exchanged? Classical cryptology requires the exchange of a key and security of the key. Classically this was done by a trusted courier. Hiring couriers to travel around the world delivering keys for thousands of perhaps very brief communications is not practical.

Diffie and Hellman’s foresight was remarkable because at the time of their paper the internet was in its infancy as a method of communication among a few military installations.

With the publication of the Diffie-Hellman paper, cryptology stepped publicly from the classical to the modern world.

Diffie and Hellman met in 1974. Simon Singh (in *The Code Book*) describes Diffie as "an itinerant cryptographer." Hellman was a professor at Stanford.

In the introduction to their paper, they set forth their problems. They have anticipated the internet which will permit world-wide communication and commerce among people who have never met. The two problems this form of communication will cause are:

1. How to prevent eavesdropping.
2. How to guarantee that messages are legitimate.

Here is a bit of the introduction to their paper; remember, this was published in 1976 – long before the internet.

We stand today on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high

grade cryptographic devices down to where they can be used in such commercial applications such as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing the ancient art into a science.

The development of computer controlled communication networks promises effortless and inexpensive contact between people or computers on opposite sides of the world, replacing most mail and many excursions with telecommunications. For many applications these contacts must be made secure against both eavesdropping and the injection of illegitimate messages. At present, however, the solution of security problems lags well behind other areas of communications technology. Contemporary cryptography is unable to meet the requirements, in that its use would impose such severe inconveniences on the system users, as to eliminate many of the benefits of teleprocessing.

Key Distribution

Cryptography requires that sender and receiver exchange a key. How do you do that over long distances, between people who have never met? Various methods have been used over the years to distribute keys; e.g., sending them by special messenger and broadcasting key strings (like the spy number stations [probably] do). But, how do you do this when the sender and receiver are half a world away and have never before communicated?

Diffie and Hellman's solution to the key distribution problem was to have two keys – a public key for encryption and a private key for decryption. This was heresy. For over 2000 years, cryptology had required one key for use by both the sender and receiver.

But, classical cryptology suggests their solution. For example, sometimes the same key is NOT used for encryption and decryption. The Hill cipher is a good example. The encryption matrix is the “encryption key” and the

inverse of the encryption matrix (the key inverse) is the “decryption key.” Now, anyone who knows a bit of linear algebra knows that the decryption key can be determined if the encryption key is known, but to someone who is ignorant of linear algebra, knowing the encryption key would yield no information about the decryption key.

If your enemy did not know how to construct the decryption matrix given the encryption matrix, the encryption matrix could be made public. Senders could use it (assuming that they knew enough linear algebra to be able to do matrix multiplication) to encrypt a message to send to you. Because you know how to construct the inverse of a matrix you could construct the decryption matrix and decrypt the ciphertext. This is the idea behind public key cryptography.

The Diffie-Hellman paper suggest such a scheme – base a cryptosystem upon a mathematical procedure for which knowing the procedure does not imply knowing the inverse procedure.

This is called a **public key cryptosystem** or an **asymmetric key cryptosystem**.

So, the search was on for such mathematical procedures.

A Miss

One early public key cryptosystem was based upon the **knapsack problem**. This cryptosystem was published in 1978 by Hellman and Ralph Merkle. At this point, we will not try to develop a cryptosystem from the problem; we will just mention the mathematical problem.

Think of having a very large collection of items that can be put into a knapsack. Out of your sight, another person places some of the items into a knapsack. You are told the weight of each object, and you are told the weight of the filled knapsack. Your problem is to determine which items are in the knapsack.

The hope of the cryptographer who is basing a cryptosystem on this problem is that it is necessary to try all possible combinations (2^n possibilities where n is the number of objects) of the objects to determine the correct one – a

brute force solution. The hope of the cryptanalyst who is trying to break the system is that there is a pattern that can be exploited to find the solution without trying all possible cases.

Obviously some conditions are necessary for the problem to have a unique solution and for the authorized receiver to be able to solve the problem. Unfortunately these conditions also make it possible for unauthorized people to break the cryptosystem, and in 1982 Adi Shamir cracked the Merkle-Hellman knapsack cryptosystem.

RSA

The most famous of the public key cryptosystems is RSA which is named after its three developers Ron Rivest, Adi Shamir, and Leonard Adleman. At the time of the algorithm's development (1977), the three were researchers at the MIT Laboratory for Computer Science. Their algorithm was first announced in Martin Gardner's "Mathematical Games" column in the August, 1977, *Scientific American*. Their formal paper was published in 1978 in the *Communications of the Association for Computing Machinery*. Gardner challenged his readers to break a message included in the column that had been encrypted with RSA. His faith in the new cryptosystem is expressed in the title of the column: "A New Kind of Cipher that Would Take Millions of Years to Break." Gardner offered a \$100 prize for breaking the message. Oops! But, more about that later.

The mathematical procedures on which RSA is based are multiplication and factoring. It is easy to multiply numbers – even very large numbers, but it is hard to factor a product (just ask a high school algebra student). To break a message encrypted by RSA, it is necessary to factor a very large number. There is no known, efficient way to do that.

One-way Communications

Public key cryptography results in one-way communication. The receiver has a public (encryption) key [like the encryption matrix] which is made available to everyone who might ever want to send the receiver a message. The receiver has a private (decryption) key [like the inverse matrix] which is never revealed. Anyone may download the encryption key and send a

message to the receiver, but (if the system is well designed) only the receiver will be able to decrypt the message. [In our Hill cipher example this would mean that no one other than the receiver could determine the inverse of the encryption matrix.] For the receiver to reply to the sender, the receiver must use the sender's public key.

Public key ciphers are asymmetric key ciphers – the sender and receiver have different keys.

But, a new problem develops. With a classical cipher, if a message arrives from a sender and the message is properly encrypted, there is a reasonable assumption [assuming that only the sender and receiver know the key] that the message came from the person who “signed” it. But, with a public key cryptosystem, anyone can send a message to the receiver and sign whatever name they want. Authentication becomes a problem.

A New Attack

Public key cryptosystems must be able to survive a third form of cryptanalysis.

Recall that the most common attack that we used in earlier sections is called a **known ciphertext attack**. Cryptanalysis is based upon having a (usually quite long) chunk of ciphertext. We tried to "puzzle out" the plaintext – often by searching for patterns in the ciphertext but sometimes by brute force.

A second form of cryptanalysis that we used was the **known plaintext attack – the crib**. This is used when the cryptanalyst knows or has good reason to suspect that for some plaintext the corresponding ciphertext is known. We did this, for example, when we searched for enciphered versions of the. Often cryptanalysts look at the beginning or the end of a message for "standard, set phrases."

Public key allows a third form of cryptanalysis – the **chosen plaintext attack**. Because the encryption key is public, the cryptanalyst can encrypt messages and try to determine the encryption algorithm by comparing plaintext and ciphertext. Because everyone has access to the encryption key, the cryptosystem must be secure against the possibility that a person is able

to send enough or the correct kind of messages to be able to determine the cipher algorithm knowing the plaintext (input) and corresponding ciphertext (output). Notice that the sender will know the plaintext and the ciphertext. Classical systems are not very resistant to such attacks. Think, for example, about an affine cipher. If we sent two plaintext letters and knew the corresponding ciphertext letters, we could determine the key. A less elegant but very effective against any monoalphabetic substitution cipher would be to send the string abcdefghijklmnopqrstuvwxyz and see what the enciphered output is. Public key cryptosystems must be made resistant to such attacks.

Hybrids

Although they are secure, public key cryptosystems tend to be slow. It might take 10 to 20 seconds to print a full page. That is too long for big documents. So, usually a hybrid cryptosystem is used. A classical, symmetric key system is the primary encryption algorithm, but the encryption key is securely distributed using RSA or some other public key cryptosystem. The public key portion of the system solves the key distribution problem.

A Different Beginning

Britain's counterpart to the United States' National Security Agency (NSA) is the Government Communication Headquarters (GCHQ). One part of that agency the Communications-Electronics Security Group (CESG), which is charged with "looking after the technical aspects of keeping official information technology and communications systems safe from compromise," apparently was aware of RSA encryption in the early 1970s. Official confirmation of this was made with the release in December 1997 of the paper "The Story of Non-Secret Encryption" (written in 1987) by James Ellis, a member of CESG. Several technical papers are also public (they are available on the CESG website) including:

"The Possibility of Non-Secret Encryption" (1970)

J. H. Ellis

Describes for the first time the ideas behind public-key cryptography which the author called non-secret encryption.

"A Note on Non-Secret Encryption" (1973)

C. Cocks

This claims to be the first practical implementation of non-secret encryption.

"Non-Secret Encryption Using a Finite Field" (1964)

M. Williamson

It is claimed that this is essentially Diffie-Hellman.

"Thoughts on Cheaper Non-Secret Encryption" (1976)

M. Williamson

Details some improvements to non-secret encryption.

Exercise

1. For each of the following ciphers, comment on each of Kerckhoffs six principles:

1a. Caesar cipher.

1b. Keyword cipher.

1c. Columnar transposition cipher.

1d. Vigenère cipher.

1e. ADFGVX cipher.

1f. Playfair cipher.

1g. One-time pad.

1h. Enigma.

1i. Hill cipher.