An Overview of Public-Key Cryptology

Franck Leprévost
University Joseph Fourier, Institut Fourier
Cedex, France

Abstract

This article provides an up-to-date overview of public-key cryptosystems. First, we explain the context at the economic level, and the implications for international relations issues. Then, we describe how secret-key cryptology works with some examples (DES, Triple DES, AES). We explain the limitations of this approach and introduce the concept of public-key cryptology through further examples. Their strengths depend on mathematical problems, which we summarize. The concept of PKI (Public-Key Infrastructure) is then introduced, which shows how to combine efficiently both secret-key and public-key cryptology. One of the main issues of public-key cryptology is the possibility to construct digital signatures. All these techniques may be combined with digital watermarking and information hiding, in order, for instance, to trace data and protect owner's copyrights. All these research areas (cryptology, digital watermarking, steganography) are very active. As an example, we shortly describe a new public-key cryptosystem based on Drinfeld modules, which is patent pending.

The Echelon Network

In 1947, the governments of the United States, the United Kingdom, Canada, Australia and New Zealand signed a security pact known as the UKUSA agreement. Its intention was to seal an intelligence bond in which common security objectives were defined, and common interception procedures and facilities were organized. Its most famous achievement is the so-called Echelon network. This has been exposed in details in 1996 in Nicky Hager's book,[4] and more recently in Duncan Campbell's report for the European Parliament[2] (see also Refs. [1], [3], and [7]). It mainly works as follows: all written electronic communications (telex, fax, email) are potentially subject to an interception at one of the stations around the world (like the Waihopai station). The computers automatically search through all the messages as they arrive at the station with the help of a dictionary program, which contains words or numbers or symbols of interest. As we already mentioned in our own work for the European Parliament,[7] and in other articles (e.g. Ref. [9]), there are some problems with this approach. First, the motivations behind these facilities have dramatically changed since 1947. At that time, during the darkest days of the cold war, these facilities were supposed to provide a technological help in the fight against the communism of Staline and his immediate successors. Now, the motivation concerns the fight against terrorism, organized crime and corruption. On the other hand, in the Echelon approach, everybody is a potential target of the network, and the first problem concerns the protection of private communications. The second one is that there are techniques available in order to protect digital data against eavesdropping. More precisely, one can use cryptography or information hiding in order to communicate safely, and terrorists or criminals are aware of the existence of these techniques and may develop appropriate software for their uses, so there is a risk to spy on everybody, and actually miss the ”bad guys”. The last problem we want to state in this article is the risk that the information collected by the facilities of the National Security Agency may be used for the protection of the US industry, and that European companies may suffer from it. As a consequence, and as we strongly suggested in our report for the EP, there is a need for facilities allowing confidentiality, integrity and authenticity of data.

Safe Communications

Safe communications may be obtained through information hiding technologies or cryptology. We now shortly describe the concepts behind these technologies.

From a functional point of view, digital watermarking and steganography provide a similar facility as encryption. They both hide an information into a cover data, like for instance a picture, a video, etc. This hidden information may be designed for the protection of copyright owners, and this is actually a very active area in R&D. Or, the techniques may be used in order to send a secret message into a non-suspect cover data. In Ref. [8], we developed with our colleagues a new (and still not detectable) method allowing one to hide about 3 pages of text into a 30-seconds video sequence, proving at the same time that it is possible to communicate safely without infringing the international regulations like the Wassenaar Arrangement (successor of the COCOM). Of course, one can combine watermarking techniques with cryptographic techniques (e.g. encrypt the hidden data, or only part of it, etc); see Ref. [6] for some applications.

Cryptosystems split into two main areas: secret-key cryptosystems and public-key cryptosystems.

Secret-key cryptosystems use one secret key for enciphering and deciphering digital data. The same key is used for both purposes. Secret-key cryptosystems subdivide themselves into stream-ciphers and block-ciphers. Stream ciphers are used for instance for the secure transfer of video on the internet. On the other hand, block-ciphers proceed first to the separation of the numerical data into blocks of fixed size, and encrypt them (there are four operating modes which influence the practical implementation of the cryptosystem and the way blocks are encrypted). The most known secret-key cryptosystem is the Data Encryption System (DES), which works on 64-bits blocks and uses a 64-bit key (in fact only 56 bits out of these 64 contribute to the security of the scheme). Because of the development of the attacks on this cryptosystem (like for instance the DES-cracker), it turned out to the crypto-community, that there was a need for an Advanced Encryption Standard (AES, see Ref. [10]. The winner of the competition organized by the National Institute of Standards and Technology (NIST) and now FIPS 197 is RIJNDAEL, which works on 128-bits blocks and uses keys of size 128, 192 or 256 bits.

However, secret-key cryptosystems face some intrinsic problems. The first one concerns the distribution of the secret keys. It is necessary, in a network, to share pairwise distinct secret-keys, what is a non-trivial task as the size of the networks rises. Moreover, they do not provide digital signatures. These problems can be solved using public-key cryptosystems. In this approach, each participant has two keys. One is public (hence the name of these systems), and allows everybody to communicate with its owner. This public key is mathematically related to another key, which is kept secret by its owner. Moreover, it should not be possible in practice to reconstruct the secret key with the knowledge of the public key (or even of chosen encrypted data with the public key). This secret key is used by its owner to decrypt the messages that have been encrypted with the corresponding public key. It is suggested to combine the public-key and the secret-key approaches into a Public-Key Infrastructure (PKI). Indeed, public-key cryptosystems are in general about 1000 times slower than secret-key cryptosystems. So, it is appropriate to first use public-key cryptosystems to proceed to a key exchange or a key agreement for a secret key of the AES, say. After this procedure, one may forget the public-key procedure and communicate safely with the AES, using the common key that has been selected. One may as well digitally sign numerical data using public-key cryptosystems: the signer uses its private key in order to sign the (hash-value of the) data. Anybody, including a judge, may verify the validity of the signature using the public-key of the owner. Of course, the schemes should pay attention to lots of attacks, and the PKI should be designed very carefully.

The security of public-key cryptosystems is based on mathematical problems, and we describe now some of them, selected into the standard IEEE-P1363 (see Ref. [5]). The Integer Factorization Problem (IFP) is the first mathematical problem which is relevant for cryptography, and the cryptosystems RSA and of Rabin-Williams are based on it. The IFP simply says, that it is ”easy” to compute n = pq, whereas it is ”hard” to recover the prime numbers p and q, knowing their product n. The Discrete Logarithm Problem (DLP) expressed in the group of non-zero elements of a finite field is the source of several cryptosystems (DSA, key exchange of Diffie-Hellman, coding methods of El Gamal, digital signatures of El Gamal, Schnorr, Nyberg-Rueppel, etc). Its version for elliptic curves (ECDLP) admits analogous cryptosystems. In fact, one may express the DLP in any cyclic group. The reason why one cares about elliptic curves (or more generally abelian varieties) comes from security considerations: sub-exponential methods have been developed for the resolution of the IFP and of the DLP in the group of non-zero elements of a finite field, but there are (to date) only exponential methods for the general resolution of the ECDLP for an elliptic curve defined over a finite field. In practice, this means that one needs only a modulus of size 163 bits using elliptic curve cryptography to achieve the security level provided by RSA-1024 bits. This is both an advantage with regards to the size of the keys, and the speed of the computations. Moreover, a moderate enhancement of the size of the parameters in the elliptic curve setting will provide the security of RSA with a much bigger modulus.

Other Cryptosystems

Still, it is important to further study and discover new public-key cryptosystems and new underlying mathematical problems: a security dogma asserts that it is not a good idea to put all the eggs into the same bag!

Only a few other cryptosystems have been discovered and studied in the recent years. Among them, one can mention NTRU, whose security is based on the lattice reduction problem, or some proposals using the braid groups in topology, or the class group of real quadratic fields in algorithmic number theory. In Grenoble, our team developed a new (patent-pending) approach based on Drinfeld's elliptic modules.[11] These are very sophisticated mathematical objects at the frontier between number theory and algebraic geometry, used for instance (in a more general setting) by Lafforgue in his proof of the conjectures of Langlands, for which he obtains in summer 2002 the highest mathematical prize, namely the Field medal. Our prototype uses a key of length 26000 characters (for a security equivalent to RSA-1024), and our implementation encrypts a 160-bit size data (which is intermediate between the key sizes used by the AES, but is the length of the hash-value of a file, using SHA-1 or RIPEMD-160) in less than 1/100 sec on a Pentium 700 MHz, the decryption is immediate.

Conclusion

The current context of international relations and business shows the importance of secure communications, and the need to rely on well designed public-key infrastructures. This is necessary for companies which want to protect their technological know-how, and their commercial strategies. This is important for governments for the protection of their military or diplomatic communications. The big actors (governments, big companies) should use cryptosystems based on several mathematical problems as a matter of risk management. Finally, in our opinion, the fight against terrorism and organized crime should integrate the de facto component of secure communications, and try to survive with it. The only way is to support the research in these areas, and development of cryptanalyze facilities on a legal basis.

References

1. Nicos Bogonikolos, Development of surveillance technology and risks of abuse of economic information. Part 1/4: The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception. European Parliament, Directorate General for Research, Directorate B, STOA Program (1999)
2. Duncan Campbell, Development of surveillance technology and risks of abuse of economic information. Part 4/4: The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadland multi-language leased, or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition. European Parliament, Directorate General for Research, Directorate B, STOA Program (1999)
3. Chris Elliot, Development of surveillance technology and risks of abuse of economic information. Part 2/4: A consice survey of the principal legal issues and instruments under international, European and national law. European Parliament, Directorate General for Research, Directorate B, STOA Program (1999)
4. Nicky Hager, Secret Power, Craig Potton Publishing (1996)
5. IEEE-P1363 draf, version 13, http://grouper.ieee.org/groups/1363/index.html
6. Martin Kutter, Franck Leprévost, Symbiose von Kryptographie und digitalen Wasserzeichen: Effizienter Schutz des Urheberrechtes digitaler Medien, Tagung des BSI (1999)
7. Franck Leprévost, Development of surveillance technology and risks of abuse of economic information. Part 3/4: Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues. European Parliament, Directorate General for Research, Directorate B, STOA Program (1999)
8. Franck Leprévost, Raphael Erard, Touradj Ebrahimi, How to bypass the Wassenaar Arrangement: A new application for watermarking, 8th ACM International Multimedia Conference on Multimedia and Security (2000)
9. Franck Leprévost, Bertrand Warusfel, Echelon: origines et perspectives d'un débat transnational. AFRI (2001)
10. http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html
11. Rolland Gillard, Franck Leprévost, Alexei Pantchichkine, Xavier Roblot, Modules elliptiques de Drinfeld en cryptologie, Comptes-Rendus de l'Académie des Sciences de Paris, To appear (2003)

Biography

Franck Leprévost is full professor at the University Joseph Fourier (France), where he teaches cryptology and mathematics. He was one of the four experts mandated by the European Parliament for the now so-called Echelon study on electronic surveillance. He is currently involved in another expertise for the EP regarding security techniques for digital media (CD, DVD, digital content on the Internet). He was one of the experts in charge of the worldwide standard IEEE-P1363 on public-key cryptography. He is consultant for several companies, organizations, and venture capitalists in Europe. He speaks fluently French and German as well.