ESTABLISHED WAYS TO ATTACK EVEN THE BEST ENCRYPTION ALGORITHM

Alexandru Tăbușcă[1]

Abstract

Which solution is the best – public key or private key encryption?

This question cannot have a very rigorous, logical and definitive answer, so that the matter be forever settled ☺. The question supposes that the two methods could be compared on completely the same indicators – well, from my point of view, the comparison is not very relevant. Encryption specialists have demonstrated that the sizes of public key encrypted messages are much bigger than the encrypted message using private key algorithms. From this point of view, we can say that private key algorithms are more efficient than their newer counterparts. Looking at the issue through the eyeglass of the security level, the public key encryption have a great advantage of the private key variants, their level of protection, in the most pessimistic scenarios, being at least 35 time higher.

As a general rule, each type of algorithm has managed to find its own market niche where could be applicable as a best solution and be more efficient than the other encryption model.

Keywords: Encryption, decryption, key, cryptanalysis, brute-force, linear, differential, algebra

Today, when almost everyone is using a computer or some sort of a cousin of it, the issues of data security are more important than ever. We keep huge amounts of data on our different personal systems (desktop PCs, laptops, tablets, smartphones, PDAs, audio players, digital recorders, electronic readers etc.) and all of it can be very easily available to many people. To consider even further, today almost every computer and electronic device is online on the internet. Some countries even see the internet as a “right” related to the freedom of information and Finland has even made a law for officially granting internet access to every citizen of the country [1. Tabusca, Silvia Maria, 2010]. These online surfers are not always aware that their personal data and information are accessible to some other “specialized” web surfers, which can retrieve the data from someone else’s machine. Of the most widely used method to protect your data is to encrypt it; we encryption systems on at least two levels: for data encryption and for transmission encryption. Inside this paper I will try to develop a bit about the history of the main two encryption systems: the private keys and public keys based one.

Private keys cryptography is perfectly adapted for encrypting large amounts of data. This model is considerably faster than the other solutions and, as a bonus, is not susceptible to cryptanalysis attacks based on encrypted chosen text.

[1] Lecturer, PhD, School of Computer Science for Business Management – Romanian-American University; e-mail: alextabusca@rau.ro

The encryption, and digital signing, algorithms based on public key systems have managed to find a broader array of uses, such as encryption keys management, sensitive data transfers, secure transmissions protocols. Moreover, during the last several years there have been quite a lot of researchers trying to improve the public key algorithms speed. One of the most promising and usable possibilities is related to the advancements in the hardware parts, mostly those processing units developed primarily for graphics use. By the use of CUDA[2] for example, all encryption operations and processes could be performed a lot faster. Many modern computer systems nowadays include a powerful GPU which runs idle most of the time and might be used as a cheap and instantly available co-processor for general purpose applications, including encryption operations [2. Pirjan, 2010]. Nevertheless, to be fair, the same advancements can also be used in correlation with the symmetric encryption processes and as a result the speed gain of the asymmetric algorithms is really just a plus when compared to older variants of the same type of algorithms and not when compared directly to their symmetric counterparts.

From the beginning, I think that I have to mention the two most important scientific branches that developed in the field of cryptanalysis during the last decades. The first branch, and the most important one, is called differential cryptanalysis. This technique can be used to attack any type of block cipher. The technique uses, from the beginning, two blocks of clear text which differs from one another only by a few bits and then studies what happens after each iteration of the encryption process. In most cases some combinations appear more often and this fact conducts to a way of developing a probabilistic attack.

The second branch, although of a somewhat lesser importance, is known as linear cryptanalysis. Using this scientific method the venerable DES[3] algorithm can be hacked with only 243 known clear texts. This technique works by the use of XOR combinations of specific bits from the clear text and the encrypted text in order to generate one bit. When this process is repeated, half of the bits are set to 1 and the other half to 0. However, quite often, the ciphers induce a deviation in one direction or another and this deviation, although small, may be exploited to reduce the workload factor.

As a conclusion that must be clear, all DES encryptions could be quite easily hacked by means of using just powerful computers available to the public in any respectable IT shop. Unfortunately, even today, there are about 28 percent of banking operations that involve encryption standards still using different forms of DES implementations.

Private key algorithm attacks

Over time there were developed and published quite a lot of classifications for organizing the attacks on private key algorithms. After a careful study of these many different classifications I think that these type of attack can be sorted in only four main categories:

1. Differential cryptanalysis attacks
2. Linear cryptanalysis attacks
3. Week key attacks
4. Algebraic attacks

[2] CUDA – Compute Unified Device Architecture is the computing engine of the Nvidia graphics processing units that is accessible to software developers through variants of industry standard programming languages

[3] DES – Data Encryption Standard; first encryption algorithm used as standard by the US government institutions

1. Differential cryptanalysis attacks

These techniques had been introduced by Sean Murphy in a case of an attack on the FEAL-4[4] algorithm and have been later upgraded by Eli Biham and Adi Shamir during an attack on the DES algorithm. These attacks practically analyze two different message encrypted with the same key. Through a very thorough analysis one can assign different probability factors to each possible key, managing to finally identify the key with the highest probability as the correct key for decrypting the message.

This type of attacks has already been used against most private key algorithms. However, against the DES there were no notable successes, as the DES has a very efficient S-BOX design, an element that holds a real barrier against this kind of attack. The greatest success was achieved by these attacks when used against the hash functions.

2. Linear cryptanalysis attacks

This type of attacks was first used by the Japanese cryptographers Matsui and Yamagishi, during an attack directed against the FEAL algorithm. Matsui also build up an attack against the DES algorithm using the same technique.

This class of attacks is comprised in the broader category known throughout the field as “known clear text attacks”. The method involves the use of linear approximation in order to describe the encrypted block’s behavior. Given enough “clear text” – “encrypted text” pairs at the attacker’s disposal, he can obtain enough elements to discover the key.

Cryptographers Langford and Hellman introduced a variety of this attack, called differential-linear cryptanalytic attack – in fact a hybrid of the first two attack categories.

3. Week key attacks

The “week keys” are encryption keys in case of which the encrypted block shows special regular properties during the encryption process or, in other cases, or displays a very low degree of security obtained through encryption. For the DES algorithm there are four known keys for which the encryption process is identical to the decryption one; a double encryption process applied to a message will provide the clear message directly.

In cases of the known algorithms the week keys, such as for example are DES or IDEA[5], do not induce much of an issue. The number of week keys is infinitesimal in comparison with the number of the possible keys, making their use very easily controllable. However, for other algorithms this problem gets bigger, the number of week keys can be considerably larger and the week parts of the encryption process can also appear in some other different forms.

4. Algebraic attacks

These attacks are based on a series of techniques of very high mathematical level. The philosophy of these attacks considers that that process of “encryption with one key and decryption with another key” is analog to the process on encrypting the same initial message with another key. This theory argues in fact that an eventual multiple encryption with the same key is obsolete.

[4] FEAL – Fast Data Encipherment Algorithm; algorithm proposed as DES alternative in 1987, by Akihiro Shimizu and Shoji Miyaguchi from NTT (Nippon Telegraph and Telephone Corporation)

[5] IDEA – algorithm published in 1991 by James Massey and Xuejia Lai. The algorithm was meant as DES replacement and was initially called IPES (improved PES) as it is a development of the former PES algorithm (Proposed Encryption Standard)

These attacks have acquired quite a level of success against about 86 percent of the widely used private key algorithms but the main one, the DES, has managed to resist.

Although the old and venerable DES algorithm has been officially "retired" in 2001 by the NIST[6] and replaced with the new AES[7] algorithm, almost ten years later we can still find a lot of applications and process that rely on the good old DES. Truth be said, most DES uses are based on a upgraded version; the today use is based on the 3DES (triple DES) solution. This solution was ratified by the official retirement of the NIST's FIPS 46-3 specification (the DES) and the approval by the same NIST of the use of 3DES solutions for US sensitive government information up to the 2030 year.

At this time, ten years after the official publication of the DES heir - the AES (as FIPS-197), I think a bit of history about the DES is in order. This algorithm has changed history and is considered the main catalyst for the academic study of cryptography.
"DES did more to galvanize the field of cryptanalysis than anything else. Now there was an algorithm to study[8]".

During the long period of time that the DES was the real standard for encryption based security there were a lot of attempts to hack it. Some of the most important and famous ones are summarized below.

The Chinese Lottery
Arguably the most innovative idea for hacking the DES algorithm. For this project, each radio and TV set in China should have been equipped with a specialized DES decrypting chipset capable of making around 1 million encryptions/second. Supposing that every one of the 1.2 billion of people in China has a radio, the Chinese government just shares the encrypted message throughout its population and the 1.2 billion chipsets are beginning to work on the decryption process. Each chipset works in its own key space and, in no more than 60 seconds, one or more keys are to be found. The conclusion was that the DES use was not sure anymore but there was quite a simple solution to avoid this matter. Even though 2^{56} equals a not so imposing 7×10^{16} (the number of possible keys for the standard DES), the 2^{112} equals a somehow more impressive 5×10^{33} number of possible keys – for just using the DES twice. Even one billion DES chipsets executing 1 million operations per second would require 100 million years in order to verify each key in a 112 bits space. So, the simple use of the DES twice on each message, with two different 56 bits keys, would make the security increase by a large factor.

Meet in the middle
Two well-known cryptographers, Merkle and Hellman, have developed a method, in 1981, that cast a shadow over the double encryption process. This method is called "meet in the middle". The theory supposes that someone has encrypted twice a series of cleat text blocks,

[6] NIST – National Institute of Standards and Technology; US institution with international influence in the field

[7] AES – Advanced Encryption Standard, sanctioned by NIST in 2001, after an international competition set up for finding the DES heir

[8] Bruce Schneier – one of the most famous cryptography specialists from the US, publisher of the "Applied Cryptography" book – considered a starting point for the study of the field of cryptography

using the electronic code book mode. For several values of the "i" index, the cryptanalyst has the pairs (P_i, C_i) where:
$C_i = E_{k2}(E_{k1}(P))$

If we apply the decryption function D_{k2} for each member of the equation we shall have:
$D_{k2}(C_i) = E_{ki}(Pi)$

because the encryption of x and the decryption of x with the same key give the same x value.

The "meet in the middle" attack uses this equation in order to find out the DES keys, K_1 and K_2. The process can be present like this:

a. We calculate $R_i = E_i(P_1)$ for all the 2^{56} values of i, where E is the DES encryption function. These array is sorted ascendant after R_i
b. We calculate $S_j = D_j(C_1)$ for all the 2^{56} values of j, where D is the DES decryption function. This array is sorted descendant after S_j
c. We go through the first array looking for a R_i that matches a S_j from the second array. When such a match is found we have a pair of keys (i,j), so that $D_j(C_1)=E_j(P_i)$. The i is a potential K_1 and j is a potential K_2
d. We verify that $E_j(E_i(P_2))$ equals C_2. If so, we test every other pairs of (clear text, encrypted text). If not, we continue to look and test the matches between the two arrays that we built before.

Of course there will be enough false alarms before finding the right keys but, in the end, these are going to be found. The attack requires 2^{57} operation (decryptions or encryptions), considerably less than 2^{112}. However, we also need a total of 2^{60} bytes of memory for the two arrays, fact that has a negative effect on the applicability of the method. Merkle and Hellman managed to make different optimizations and compromises that finally produced a version of the method that involves a much smaller amount of memory required. Taking into account this type of attack the DES lost the edge that was provided by the double encrypting mechanism.

COPACOBANA[9]

In 2006, even though the DES was already replaced theoretically, the algorithm was still very much in the focus lights of the academic world. The universities of Bochum and Kiel, both in Germany, organized an experiment for breaking the DES encryption.

They built a special parallel machine, with parts and components amounting to only 10000 USD, that managed to crack a DES encrypted message in 9 days. During the following year the two universities continued to improve on the software side of the machine and, after one year, the time required for the DES break shrunk to 6.4 days.

Closer to our time, in 2008, the SciEngines GmbH company, developed by the two initial partners of the COPACOBANA project, has brought about a new version of the machine, called COPACOBANA RIVYERA. This new equipment was able to decrypt DES messages in less than one day.

With the official adoption of the new standard encryption algorithm by the NIST in 2001, the AES, a new target appeared on the scene of cryptography. Most attacks shifted during the

[9] COPACOBANA – the acronym comes from the phrase "Cost-Optimized PArallel COde Breaker"

following years from DES (and its diverse universe of variants) to the new AES. This algorithm, also known as Rijndael, has attracted more and more attacks… fortunately with little success, at least up to now.

The AES algorithm is largely used in two forms: 128 bits blocks with 128 bits keys or 128 bits blocks with 256 bits keys. A 128 bits key permits a keys space of 2^{128} (2 x 10^{38}) variants. In case someone builds a dedicated machine for breaking this cipher by using one billion chipsets, each one capable or evaluating a key every picosecond, it would take approximately 10^{10} years to go through the entire keys space.

Despite its complexity, AES – as its DES predecessor too, is a mono-alphabetic substitution cipher. Every time a certain clear text block enters in the encoding process the same encrypted text goes out. Mathematics specialists think that ultimately an attacker could exploit this propriety in order to break the AES. The algorithm is considered by NIST to be safe as standard up to 2020-2030 at most.

Public key algorithm attacks

Even though these public key algorithms are considered more “fashionable” and modern than the private keys ones, they are also vulnerable to different types of attacks. One of the most widely used public keys algorithm today is known as RSA[10]. These algorithms are based on the mathematical problem of factoring very large numbers[11]

In 1991 the RSA Data Security company launches the RSA Factory Challenge in order to test its own encryption system.

The RSA contest offered a 155 digits number to be factored by contestants for a cash prize. In 1999, after eight years, RSA got their first winner (he made the calculations in no less than seven months).

During the period of 1991 and 2007 the RSA Challenge was open and there were 54 numbers listed by the RSA company for the contest. The contest became inactive in 2007 but anyone interested is still welcome to try and factor the numbers. Up to the beginning of 2011 only 16 of the numbers were factored. The last one was “broken” in December 2009 by a dedicated team of researchers from six institutions, led by T.Kleinjung.

The most difficult challenge was considered the RSA-2048 number, with no less than 617 decimal digits. All specialists of the field agree that this number will not be factored for the next decades unless spectacular knowledge is developed in the fields of mathematics (integer factorization) and electronics (computational power breakthroughs).

At the ending of the paper, as a personal conclusion based on many years of experience in the field and on extensive use of many security and encryption applications, I advocate the use of both types of algorithms depending on the target and environment. The best solution for encrypting large data collections is still the one based on private key algorithms – with the use of AES of even the older 3DES; their speed and size of encrypted data give them their edge in this type of environment. For the use of instant encryption systems (for messaging, electronic signatures, data transmissions etc.) I argue for a public key algorithm implementation, best based on the RSA solutions.

[10] RSA – the acronym comes from the algorithm authors: Ron Rivest, Adi Shamir and Leonard Adleman, all from MIT (Massachusetts Institute of Technology)

[11] Factoring – means representing a number as the product of prime numbers

1 References & Bibliography

- Boneh, D – “Twenty years of attacks on the RSA cryptosystems”; published in “American Mathematical Society”, vol.46 no.2 – 1999, pages 203-213
- Diaasalama, Abdul Kader; Mohiy, Hadhoud – “Studying the Effect of Most Common Encryption Algorithms”; published in “International Arab Journal of E-Technology” vol.2 no.1 – January 2011
- Gupta, Upasana – “Bank Information Security – Top 5 Certifications for 2012”; published on www.bankinfosecrity.com – December 2, 2011; last visit on December 4, 2011
- Manavski, S.A. – “CUDA Compatible GPU as an Efficient Hardware Accelerator for AES Cryptography”; published in proceedings of “Signal Processing and Communications, 2007” conference – December 2008, ISBN 978-1-4244-1235-8, pages 65 - 68
- Shashi, Mehrotra; Rajan, Mishra – “Comparative Analysis of Encryption Algorithms for Data Communication”; published in “International Journal on Computer Science and Technology” vol.2, issue 2 – June 2011, ISSN 2229-4333, pages 292 – 294
- Thorsten Kleinjung, Kazumaro Aoki, Jens Franke and others – „Factorization of a 768-bit RSA modulus”; Workshop on Tools for Cryptanalysis, 23 June 2010; http://www.loria.fr/~zimmerma/talks/rsa768_tools2010.pdf
- Tabusca, Silvia Maria - "The Internet Access as a Fundamental Right"; published in “Journal of Information Systems and Operations Management”, vol.4.no.2, ISSN 1843-4711, pages 206-212
- Pirjan Alexandru - “Improving software performance in the Compute Unified Device Architecture”; published in “Informatica Economica Journal”, 14(4), ISSN 1453-1305, pages 30-47

2 Works Cited

[1. Tabusca, Silvia Maria, 2010] Tabusca, Silvia Maria (2010, December). "The Internet Access as a Fundamental Right", published in “Journal of Information Systems and Operations Management”, vol.4.no.2, pages 206-212, ISSN 1843-4711

[2. Pirjan, 2010] Pirjan Alexandru (2010). “Improving software performance in the Compute Unified Device Architecture”, published in “Informatica Economica Journal”, 14(4), 30-47, ISSN 1453-1305