Ed. 05-2022


www.ciphermachinesandcryptology.com

# Is One-time Pad History?

DIRK RIJMENANTS

**Abstract** Are one-time pads a thing of the past? There has been quite a bit discussion and some experts argue that one-time pad is no longer a system for today's needs, that it is impractical and creates enormous key distribution problems. They say that current computer algorithms provide enough security and public key schemes solve the problem of key distribution. This paper explains why reality is very different and why one-time pad will eventually be the only future.

**Keywords** Cryptography, One-time Pad, Manual Encryption, Cryptographic Algorithm, Public Key Encryption, Mathematical Security, NSA, GCHQ, FAPSI,

## One-time Pad Encryption

Let us first explain one-time encryption, and what this paper is about. One-time pad encryption is a most basic encryption algorithm where the readable data is combined with a truly random key of the same length as the data. The key should never be reused and always destroyed after use. The system was invented in 1917 and it is mathematically unbreakable. There is no way to crack it with current or future computer power, simply because it is mathematically impossible. The downside is that the rules of one-time use create a cumbersome key distribution with associated problems.

I must point out here that this paper is about modern one-time encryption applications, not the pencil-and-paper spy trade craft (although it is just as secure). This paper is neither about small one-time passwords or one-time keys, which are only valid for a single encryption session by some crypto-algorithm under control of that key, and the paper is certainly not about the many snake-oil applications that pretend to be unbreakable because they claim to be using one-time encryption, while they actually are not. Remember: key as long as the data, truly random and used only once. There is no way around these three conditions without messing up the unbreakable part!

Many cryptologists believe that one-time encryption is something from the past. They claim that modern encryption algorithms offer secure communications and privacy, that the current key exchange schemes solve the complex key distribution and that there is no longer a need for one-time encryption. This paper explains why they are wrong and why they don’t admit that.

## Insecure Systems

For a start, there is the problem of implementing secure systems. A strong encryption algorithm is useless on a computer that contains viruses or spy ware that captures your keystrokes or retrieves your data before it is encrypted. Today, virtually all computers are vulnerable to attacks, and most computers are actually infected, especially those connected to an external network like the security nightmare called 'the Internet'.

The modern Personal Computer is a true security disaster, everything leaks out, and anyone can get in. In fact, today, all our means to communicate are completely digitalized and automated, but at the same time, we no longer have any control over these systems. We have no idea of what our own computer is doing, which processes are running in the background, or what plug-ins, add-ons and other unidentified software is downloaded automatically to “stay compatible”. This is a most dangerous evolution which has gone way too far already.

There are strong algorithms available, but we use completely insecure computers. Even firewalls of government agencies have proven to be vulnerable to attacks. In 99 percent of cases, Intelligence agencies don't have to break any encryption, they simply retrieve the information before it is encrypted. That is why the only truly secure encryption is performed by dedicated crypto devices or computers, well separated from the outside world. Cryptologists or software designers who claim that their software provides secrecy and privacy on your personal computer really do not know what they are talking about, not because of incompetence, but simply because they really have no idea of all the processes that are running on your computer. Actually, nobody has any idea.

## Mathematical Security

Unbreakable encryption has been available since the 1920s. However, failing to solve the key distribution issues of one-time pad encryption, cryptologists turned to public key cryptography in the 1970s to share short secret keys of symmetric algorithms. Modern symmetric block ciphers and stream ciphers, in combination with asymmetric public key algorithms, replaced one-time pads for secure communications because of practical considerations and their solution to key distribution.

Modern computer algorithms have done a great job in protecting Internet communications and e-commerce in the past few decades. Today, traditional symmetric block ciphers and stream ciphers, under control of a secret key, still encrypt vast amounts of data that travels around the world, but asymmetric public key cryptography enables a secure exchange of the secret symmetric keys. It’s an all-in-one automated package: the data is encrypted with a symmetric algorithm under control of a random secret key. That secret key is encrypted with the asymmetric public key that is available to everyone. The whole package, encrypted data and encrypted secret key, is sent to the receiver. He decrypts the secret key with his private key and uses that secret key to decrypt the actual data.

Problem solved? Not really. As before, all data is still encrypted with traditional symmetric algorithms (public key cryptography is too computation-heavy for large data and is used only to encrypt short keys). Man-made symmetric algorithms, with all their known and unknown design flaws, poorly computer-generated random for keys and weak key schedules that compromise public key implementation, running on today's insecure personal computers, are a disaster waiting to happen. Some of these flaws are requested or even imposed by governments to enable eavesdropping in the name of their nation's security. Recently, it became clear that some organisations pre-compute frequently used prime groups, thus bypassing the near impossible task of prime factorization, used for public key cryptography. The result is that current crypto algorithms and communications security are, at best, reasonable secure. Digital security and privacy no longer exist.

## Trusting Algorithms

Can we even trust any symmetric crypto algorithm? All currently used algorithms are openly examined and tested in the public. But there are other players than the public. Government agencies have far more resources, technology and knowledge than the public. It is known that agencies such as the NSA, GCHQ, FAPSI or the FSB Academy have an unmatched collection of brain power, money and computational power.

Are the current algorithms really unbreakable, or at least rather strong? In both the US and Russia, two key players in the world of cryptography, the use and export of cryptography is approved and controlled by the government. In the US, cryptography export is legally regarded as weapons export, and Russia forbids using non-approved cryptography.

On what basis do they approve or forbid the use or export of a new algorithm? Do they only approve weakened versions of an algorithm? Why do they lower key sizes of algorithms? A simple question gives you the answer: would they cut in their own throats, and approve and spread unbreakable encryption and deprive themselves of their primary job, collecting information?

Now you will ask, why don't we prove that those algorithms are breakable? Well, we all know what we need for that: huge budgets and resources, and governments have them. You also need very capable people, and guess who has most of them, and the money to recruit them? Indeed! That's not paranoia from our side, that's efficient pro-active management and safeguarding sources from their side.

Current crypto algorithms provide hardly any security or privacy. Some experts argue that modern algorithms are practically unbreakable. Ask any cryptologist to provide the mathematical proof that his algorithm is unbreakable. He simply cannot. Even if they do not find a way to break something, it’s not unbreakable. They have only proved they cannot break it themselves, or claim they cannot break it, but of course won’t tell you. They can claim their encryption, at best, pretty strong. Nothing else. A good old quote of NSA’s David Boak says it all.

*"The ‘approved’ systems have simply been shown to adequately resist whatever kinds of crypto-mathematical attacks we, with our finite resources and brains, have been able to think up. We are by no means certain that the [opponent] equivalent can do no better"*.

So, we’ll just have to trust them and hope no one is smarter or has better computers. Can we trust them? Do you prefer trust and hope, or do you prefer proof? Use your common sense!

## Long Term Security

If an algorithm seems safe today, will it be safe tomorrow? No single computer developer could have imagined 40 years ago that we would have computers with a speed of 1.105 Peta Flops, that's $1.105*10^{15}$ or 1.105 quadrillion floating point operations per second (this record is probably already broken when you read this). Nothing is unbreakable, except for one-time pad. Therefore, we make algorithms that take so much time to break, that the information will be useless by the time we decrypted it. Actually, we are talking here about the time, required for a brute-force attack on the key, because we can't predict if or when some smart guy finds an efficient cryptanalytic attack to shortcut the job. That is how all current cryptography works.

However, Intelligence agencies collect and store huge amounts of possibly interesting data traffic for the future. If new technology or cryptanalytic techniques enable the decryption of these archives, this can have devastating consequences. Imagine critical information about important people, operations or political decisions, decrypted after 20 or 30 years. Many of the involved people would still be alive or even in office.

On the other hand, a one-time pad encrypted message will never be broken if the keys have been destroyed. Just take a look at the past. Messages that were encrypted in the 1950's with 'state of the art' cipher machines and were kept archived by the adversary (which actually happened) are now generally broken within a few seconds, minutes or some hours at the most. Let's hope for them there wasn't anything crucial to hide. The messages that were sent 50 years ago with a one-time tape device such as the ETCRRM or ROCKEX will stay unbreakable for ever.

**The Future of One-time Pad Encryption**

All kind of flaws are already exploited today on a huge scale by few organizations. Unfortunately, governments that weaken domestic encryption make their country and infrastructure also vulnerable to hostile foreign states, which is always a very bad idea, regardless any excuses that government presents for doing so.

Inevitably, the technology to exploit flawed encryption technology will find its way to more people, including criminals, on a larger scale in the near future. This will cause a complete collapse of all secure communications, privacy, e-commerce and the global monetary system. Unfortunately, recovering from such a crypto collapse will take a very long time. The current infrastructure of network technology, servers and computers is technically unsuitable to provide real security and privacy. It will take quite some time and effort to change that infrastructure.

Information theory taught us that only a truly random key, as long as the message, will enable encryption that resist cryptanalysis. Any key that is shorter than the message, regardless how random it is, will eventually provide the clear and unique solution to breaking the message. This is a mathematical fact. In the end, only perfectly secure encryption will survive the evolution of cryptography. Just as classical pencil-and-paper ciphers were rendered useless with the advent of the computer, so will current computer based crypto algorithms become victim to the evolution of technology.

Has one-time pad encryption a future? Of course, because it is the only crypto algorithm that has a future! Once the codebreaking technology has surpassed the capabilities of cryptologists and the limitations of mathematics to make strong encryption, there will no longer be any crypto algorithm that survives the evolution of cryptology, unless it meets the standards of information-theoretical perfect security. Only one-time pad encryption will therefore survive that evolution. Technology and science, instead of cryptologists, must then provide a solution to the key distribution issues. This can be some modern high-tech version of the briefcase with handcuffs or quantum key distribution which is already in use today. One way or the other, one-time pad encryption and a system to distribute its keys, practical or impractical, will be implemented in the future because we will have no other choice.

**Practical Solutions**

How could such a secure network look like? One possible and practical setup is a multiple star-topology with interconnected nodes. Each user connects to his own node. All data or e-mail traffic between the connected user and the node is encrypted with his user-node one-time pad key, which is destroyed immediately after use. The user's node automatically decrypts the data he sent, re-encrypts it with an inter-node key and sends the data to the receiver’s node. All data traffic between the different nodes in the network is also one-time pad encrypted with unique random inter-node keys for each node connection. The receiver's node decrypts the data, re-encrypts the data with the key that the node shares with the receiving user and sends it to him. If any user is not connected to his own node, then his encrypted data will be relayed automatically via other nodes to his own node for further processing. We can also provide authentication by

calculating a hash value from the plain data. The hash value should be encrypted together with the data. Any corruption or manipulation of the encrypted data will cause a difference with the proper hash value. Thanks to the unbreakable encryption, only the proper sender can create the correct hash and only the proper receiver can verify the inserted hash value.

This way, each encryption process has used its own truly random keys, and there's no mathematical relation whatsoever between any of the data that travels across the various network connections. Moreover, the user doesn't need a separate key for each correspondent and the generation and distribution of keys is all done locally. This principle is basically identical to the system of interconnected one-time pad encrypted teletype nodes, in use from the 1950s until the 1980s, albeit much faster, with many more users and faster production of keys. The arguments by some cryptologists that one-time pad encryption would require an exponential amount of keys to connect all users (a key from everyone to everyone) is a fairytale, already solved half a century ago with communications nodes. We just need to modernize that perfectly secure system.

**Distributing One-time Pad Keys**

Some cryptologists still argue that the distribution of large quantities of one-time pads or keys is impractical. This was indeed the case in the era of paper one-time pads, punched one-time tape reels, 1.44 MB floppy disk or 100 MB disk drives. However, today's hardware is capable of generating huge amounts of truly random keys at very high speeds, and one-time encryption software, which requires virtually no computational effort, can process large quantities of data at very high speeds. Current data storage technology enables the physical transport of enormous quantities of truly random keys on very small devices.

The generation and distribution of keys for node-user and inter-node connections can be fully automated. One solution for secure distribution of one-time pad keys is quantum key distribution (QKD). This technology enables perfectly secure transmission of key bits over fiber optics. SECOQC in Vienna, Austria, was in 2008 the first ever QKD protected network. The current DARPA Quantum network connects ten nodes. ID Quantique, QuintessenceLabs and SeQureNet are some of the commercial firms that offer QKD networks. The perfect one-time pad encryption is the ideal partner for the perfect quantum key distribution.

However, even with current random generation and data storage technology it would be technically possible to physically supply enough random keys physically between nodes. Providing random keys to all users that are not connected to a QKD network is more challenging but not impossible, and if technology can't find a solution, there's still the option to distribute the end-user keys physically. This will be the price to pay for security, but doesn't have to be a real problem. The effort to distribute those keys can be quite minimal.

The user would have to go to his local node and receive, after identification, his local generated one-time pad keys on some type of data carrier. This process should be fully automated. The method is comparable to withdrawing money from your ATM. With such a co-called sneaker net, the transfer of data on removable media by physically couriering, you can reach a throughput (amount of data per time unit) of random key material that is greater than what a network can process on encrypted data. In other words, it could take some time to transport a Terabyte of truly random keys, but it will take a long time to consume that amount on a broadband network. A terabyte sized key can easily encrypt you e-mail traffic for a year, including attachments. Many Internet providers won't even allow this amount of traffic. Driving once a year or every few months to a node terminal to collect your own random key is an acceptable effort to obtain absolute security.

One-time pad encryption will provide absolute security and privacy to all users, but will also deprive all governments from their eavesdropping capabilities and many cryptologists from their

job. The truth is that perfect secure encryption is not a mathematical problem but a technical problem that can be solved. Of course, most cryptologists don't like to hear this. The problem has been solved in the past and we can adapt it with current technology to today's requirements. It won't be easy to do the makeover, due to years of development in the wrong direction, but having that huge insecure infrastructure without real security or privacy can never justify keeping it, merely because it exists. It's a typical case of mission creep; they continue on the wrong path because they hesitate to turn back. The longer we hesitate, the bigger the disaster to come and the more effort it takes to switch over.

**Conclusions**

Public key algorithms and traditional symmetric algorithms are, at least at this moment, still useful. They have earned their place in the commercial market for reasonably secure large-scale communications. However, in many cases real security is preferred above practical considerations. We need both practical applications and secure applications, and we can favour one of them for a specific situation. We cannot compare them, nor can we pretend that we don't need the one because we have the other.

Eventually, we have no choice and will have to replace all current crypto and communications technology. This starts with creating perfect secure networks and is followed by redesigning the insecure architecture of personal computers, because it is pointless to have secure communications if the connected equipment is as leak as a sieve. The biggest challenge however will be to find a trusted authority willing to approve, support and enforce the development of secure fully automated key distribution and encryption technology that actually sidelines them. As long as governments do not understand the benefits of strong encryption for everyone, and think as far forward as the next election date, we will never regain our privacy. At this moment, most of them unfortunately tend to go towards the opposite direction, as foreseen by George Orwell.

The current precarious state of Internet security, or rather the lack of security, is where the limited use of one-time pad encryption for specific purposes comes into the play. One might have found it ridiculous in our high-tech world, if it wasn't for the disastrous state our privacy is in today. Indeed, even the pencil and paper one-time pad still provides a practical encryption system for crucial private communications where the correspondents can perform all calculations by hand and without the aid of their insecure computers and unreliable network. You could call it the poor man's one-time pad, but it works perfectly and it is the only system that we can really trust today, and the best of all, nobody will ever be able to decipher your messages, not even three-letter organisations.

Is one-time pad encryption a thing of the past? Absolutely not!

Note from the author.

The original version of this paper was written in 2009. At the time, it might have been regarded as a silly prophecy. Unfortunately, in today's post-Snowden era, reality has surpassed our greatest fears by far and secrecy and privacy have never been in more precarious position. It's everyone's responsibility to ensure that secure communications remain a fundamental basic right.