How safe is encryption today?

March 23 2015, by Ron Steinfeld

Crytography has come a long way since the days of cypher disks like this one. Credit: Gianni/Flickr, CC BY-NC-ND

When checking your email over a secure connection, or making a purchase from an online retailer, have you ever wondered how your private information or credit card data is kept secure?

Our information is kept away from prying eyes thanks to cryptographic

algorithms, which scramble the message so no-one else can read it but its intended recipient. But what are these algorithms, how did they come to be widely used, and how secure really are they?

Coded messages

The first cryptographic methods actually go back thousands of years to the time of ancient Greece. Indeed, the word "cryptography" is a combination of the Greek words for "secret" and "writing".

For example, the Spartans famously used a system where they wrapped a piece of papyrus around a staff of a certain girth, and wrote their message down the length of the staff. When the papyrus was unravelled, the message was jumbled until it reached its destination and was wrapped around another staff of the correct circumference.

Early encryption algorithms like these had to be applied manually by the sender and receiver. They typically consisted of simple letter rearrangement, such a transposition or substitution.

The most famous one is the "Caesar cipher", which was used by the military commanders of the Roman emperor Julius Ceaser. Each letter in the message was replaced in the encrypted text – the ciphertext – by another letter, which was shifted several places forward in the alphabet.

But over time such simple methods have proved to be insecure, since eavesdroppers – called cryptanalysts – could exploit simple statistical features of the ciphertext to easily recover the plaintext and even the decryption key, allowing them to easily decypher any future messages using that system.

Modern computing technology has made it practical to use far more complex encryption algorithms that are harder to "break" by

cryptanalysts. In parallel, cryptanalysts have adopted and developed this technology to improve their ability to break cryptosystems.

This is illustrated by the story of the Enigma cryptosystem used by the German military during the Second World War, as dramatised most recently in the movie The Imitation Game.

Enigma's relatively complex encryption algorithm was implemented using electromechanical computing technology to make it practical for German military communications. An extension of the same technology was used by the "bombe" machines of the British cryptanalysts to make it practical to break the cipher.

Current cryptosystems

The cryptosystems in wide use today have their origins in the 1970s, as modern electronic computers started to come into use. The Data Encryption Standard (DES), was designed and standardised by the American government in the mid 1970s for industry and government use. It was intended for implementation on digital computers, and used a relatively long sequence transposition and substitution operations on binary strings.

But DES suffered a major problem: it had a relatively short secret key length (56 bits). From the 1970s to the 1990s, the speed of computers increased by orders of magnitudes making "brute force" cryptanalysis –- which is a simple search for all possible keys until the correct decryption key is found –- increasingly practical as a threat to this system.

Its successor, the Advanced Encryption Standard (AES), uses minimum 128-bit keys by contrast, and is currently the most popular cryptosystem used to protect internet communications today.

Key problem

The AES also has limitations. Like all earlier cryptosystems, it is known as a symmetric-key cryptosystem, where the secret key is known to both the sender who encrypts the message (lets call her Alice), and the receiver who decrypts the message (lets call him Bob).

The secret key, being secret, cannot simply be exchanged over a public communication channel like the internet. If that was intercepted, that would compromise all future encrypted messages. And if you want to encrypt the key, well that produces another problem of how to secure that encryption method.

So, Alice and Bob must first use a private communication channel, such as a private meeting in-person, to exchange the secret key before they can use the cryptosystem to communicate privately. This is a significant practical hurdle for internet communications, where Alice and Bob often have no such private communication means.

To overcome this hurdle – known as the key distribution problem – an ingenious different type of cryptosystem, called an asymmetric-key, or public-key, cryptosystem was devised in the 1970s.

In a public-key cryptosystem, the receiver Bob generates two keys: one is a secret key that Bob keeps to himself for decryption; while the second is a public encryption key that Bob sends to Alice over a public channel. Alice can use the public encryption key to encrypt her messages to Bob. But only Bob can decrypt it with his private key. It thus provides a solution to the key distribution problem of symmetric-key cryptosystems.

In practical applications, due to the higher computational demands of public-key systems compared to symmetric-key systems, both types of

cryptosystems are used. A public-key cryptosystem is used only to distribute a key for a symmetric key system like AES, and then the symmetric key system is used to encrypt all susbequent messages.

Consequently, the resulting privacy depends on the security of both symmetric and public key cryptosysems in use. The most commonly used public-key cryptosystems in use today were devised in the 1970s by researchers from Stanford and MIT. They are known as the RSA cryptosystem (from the initials of the designers, Ron Rivest, Adi Shamir, and Len Adleman) and the Diffie-Hellman system, and make use of techniques from an area of mathematics known as number theory.

Strengths and weaknesses

So how secure are the AES and RSA/Diffie-Hellman systems in use today?

The security of any cryptosystem in practice depends on both its mathematical design properties (its "mathematical security"), as well as details of its implementation and use (its "implementation security"). I'll focus on mathematical security here, but I'll add that bad implementations of and misuse of cryptography has been at the root of many security vulnerabilities discovered over the years.

The mathematical security of modern AES and RSA/Diffie-Hellman cryptosystems relies on the assumption that the computational complexity of certain mathematical problems is too large to be solved in a reasonable time by attackers using current computing technology.

Although these complexity assumptions cannot currently be mathematically proved, the fact that these assumptions have been studied by the cryptographic research community for a significant time (over 15 years for AES and over 30 years for RSA and Diffie-Hellman

systems) and have remained valid, provides reasonably strong evidence for the validity of these assumptions.

Moreover, in the case of the RSA and Diffie-Hellman systems, the underlying mathematical problems are natural problems studied independently by mathematicians working on number theory.

More specifically, breaking the RSA system is closely related to the problem of factoring large composite integers into a product of prime numbers, whereas the security of the Diffie-Hellman system is based on the problem of finding the logarithm of a given integer (to a given base) modulo a given prime integer.

These two examples are problems that have been studied in number theory since at least the 18th century, yet mathematicians still have not discovered efficient algorithms to solve them. This may give us some confidence about their computational difficulty.

Nonetheless, significant mathematical improvements over the last 30 years have made such problems solvable in less time than previously assumed. This, together with the improvements in computing technology speed, has required longer keys to guarantee a given security level against the best known attack algorithms.

For example, estimated RSA key lengths for a typical security level have increased from around 400 bits in the early 1980s to more than 1,200 bits today.

So far, gradual increases to key lengths have been sufficient to compensate for problem solving computing technology advances. But it remains a real possibility that future algorithmic research breakthroughs could make systems such as RSA insecure for any practical key lengths.

For instance, in 2013, a team of European researchers found efficient algorithms to solve certain variants of the discrete logarithm problem (known as the discrete problem in finite fields of small characteristic). While apparently not applicable to the variants of the problems typically used in RSA and Diffie-Hellman cryptography, this demonstrates the fragility of the cat-and-mouse race between cryptosystem security and natural mathematical advances.

The future of cryptography

I see two potential developments which may have a major impact on cryptography.

The first one relates to the development of quantum technology. In a breakthrough theoretical result in the 1990s, the mathematician Peter Shor demonstrated the potential of a large scale quantum computer. This exploits the principles of quantum mechanics to solve the integer factorisation and discrete logarithm problems efficiently, thus rendering the RSA and Diffie-Hellman systems insecure.

While large scale quantum computing technology has not yet been realised (and prospects for its realisation remain unclear), the impact such a realisation could have on cryptography cannot be overestimated.

Fortunately, researchers already have devised two possible approaches to deal with this problem if it arises in the future. One is the development of public-key cryptosystems that are believed to be secure even against quantum computing attacks. The other is quantum cryptography, a communication technique that relies on physical assumptions and the laws of quantum physics to provide security.

The second potential development relates to the increasing usage of cloud computing. Unfortunately, unless encryption is used to protect our

stored private data, the privacy of that data from the cloud server (or any other entity having access to the cloud server data, such as a hacker) is compromised.

The use of conventional encryption algorithms by the user, on the other hand, also has the side effect of preventing the server from performing useful processing on the data for the user (e.g. to search the data). New types of cryptosystems are currently under development by the cryptographic research community to overcome this apparent paradox by allowing the server to process the encrypted data without revealing the data to the server.

As you can see, the state of the art in cryptography is currently strong enough to protect most of our email and online transactions, but its future status isn't entirely certain. The future – particularly quantum computing – may result in even stronger cryptographic systems, but also raises the prospect of new means to break them. The cat-and-mouse continues.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation