DOI: 10.24425/academiaPAS.2023.147628

Bartosz Naskręcki, PhD

is a mathematician specializing in arithmetic geometry, an expert in number theory, and an enthusiast of mathematical crystallography. He is passionate about promoting public awareness of the achievements of Polish cryptologists. In his private life, he is a happy father and husband, as well as a notorious avocado grower.

nasqret@gmail.com

The Art of Encryption

In our digitally driven era, safeguarding information has become paramount. Encrypting data is essential for keeping it safe and secure.

Bartosz Naskręcki

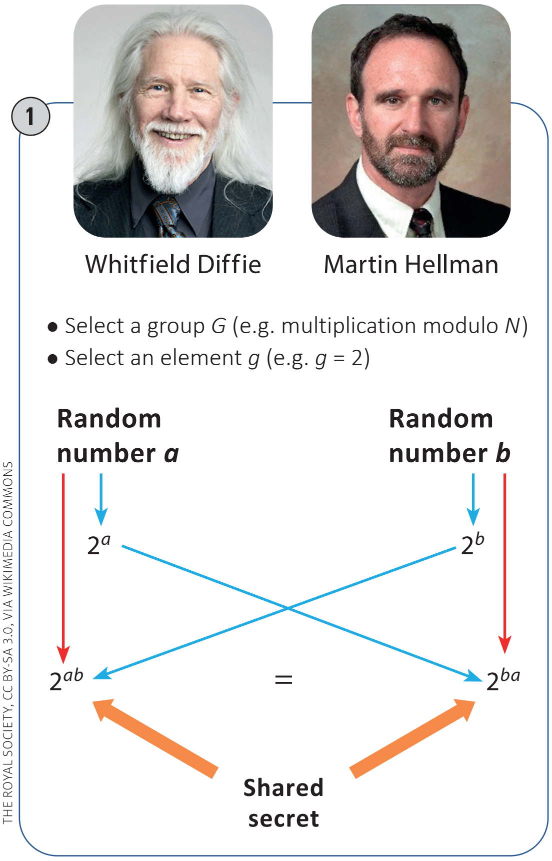
Adam Mickiewicz University in Poznań
PAS Institute of Mathematics in Warsaw

The twenty-first century is the era of information. We live our lives immersed in an unending stream of data, unparalleled in any previous era in history. To transmit all this data effectively and securely, we make constant use of highly sophisticated encryption methods. The fundamental ideas of such encryption in fact date back to ancient times.

To illustrate the basic concept of encryption, let's say we want to send a message to someone in another room: a short sentence like "I am in the next room." This information is intended for one person only. Anyone who speaks English, however, will easily understand the sentence and draw the obvious conclusions. We need a way to encode the text, but in a way that makes it easy to undo, i.e., decode the original message. We can encrypt the message using a simple method.

Let's start with a string of capital letters IAMINTHENEXTROOM (removing spaces does not pose a significant challenge to reading). We replace the letter A with B, B with C, etc., moving through all 26 letters, with letter Z changing back to A. As a result, we

LENSCAP PHOTOGRAPHY/SHUTTERSTOCK.COM



THE ROYAL SOCIETY, CC BY-SA 3.0, VIA WIKIMEDIA COMMONS
USER .:AJVOL:. ON EN.WIKIPEDIA, CC BY-SA 3.0, VIA WIKIMEDIA COMMONS

Fig. 1
Diffie-Hellman Exchange

Diffie-Hellman Exchange

Two individuals agree on a number, for instance, 2. Each of them then arbitrarily selects a secret integer, say *a* and *b*. They calculate 2^a and 2^b and send each other the result. They now compute $(2^a)^b$ and $(2^b)^a$ – in both cases, the result is equal to $2^{(a*b)}$ – and this becomes their shared secret. If the exponentiation operation is performed in modular arithmetic (that is, stated as a remainder after division by *N*), we get a result for which the task of reconstructing the original exponents *a* and *b* is extremely complex. The problem of recovering a number *a* from (2^a modulo *N*) is known as the *discrete logarithm problem*. Generating shared secrets in this way is incredibly simple and effective. It is a solution to the problem of creating a common key for block cipher exchange (Fig. 2).

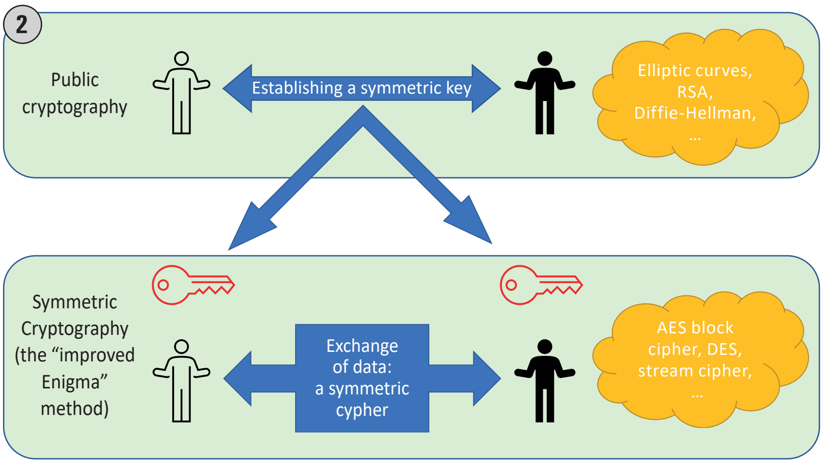

Public cryptography
Establishing a symmetric key
Elliptic curves, RSA, Diffie-Hellman, ...
Symmetric Cryptography (the "improved Enigma" method)
Exchange of data: a symmetric cypher
AES block cipher, DES, stream cipher, ...

Fig. 2
The method of encryption commonly used for webpages

get the text: JBNJOUIFOFYUSPPN. It doesn't look very intelligible, right? If we openly exchange a scrap of paper with this text written on it, even visibly to strangers in the room, no one will be able to easily read the message. How can the recipient decode the message? Simply by shifting the letters one position back in the alphabet, to arrive at the message: IAMINTHENEXTROOM.

This method of encoding information is known as a *Caesar cipher*. The Roman statesman Julius Caesar used this simple technique to conceal information from prying eyes. The most important features of this method include quick encoding of the message, reversibility of the process, keeping the message concealed from outsiders, and a small amount of information needed for encoding/decoding.

These four features in fact remain the fundamental postulates of today's information security. The essence of modern cryptography – the science of creating and breaking ciphers – is to develop procedures that meet these very same requirements and guarantee us a high level of security: in other words, guaranteeing that it is virtually impossible to read the original message without knowing a secret key.

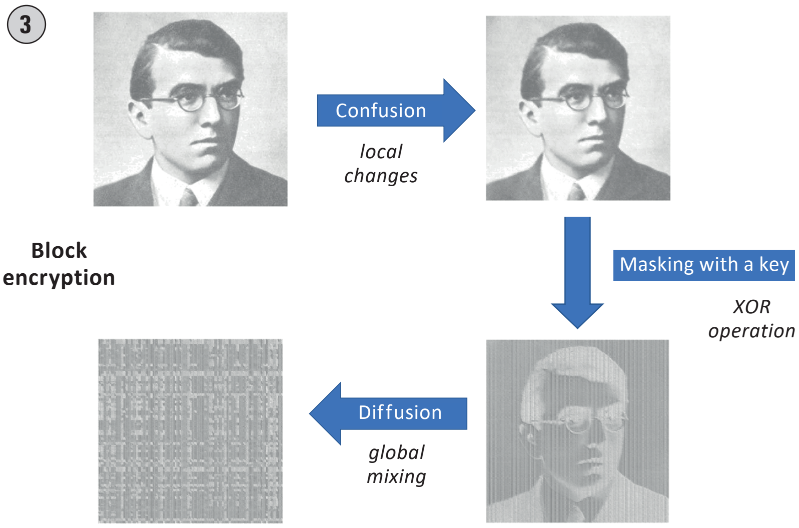
When surfing the Internet today, we no longer exchange scraps of paper with symbols written on them, but the above principles of data transmission still very much apply. Today's data-processing procedures nevertheless have to cope with sending a huge number of messages: an amount of information that can roughly be represented by a set of symbols reaching 10^{20} elements. A basic Caesar cipher is too simple to safely encode such a hard-to-imagine quantity of data.

The Middle Ages

An idea devised by Blaise de Vigenère, a French scholar from the sixteenth century, comes to our rescue here. The Caesar cipher, which involves shifting letters by a fixed number of positions, is very easy to break. For each language (English or Polish, say), we can draw up a table of letter frequencies in normal text. If we compare this to a text in the encoded alphabet, aligning the most frequently occurring letters will often enable us to easily guess by how many positions the text needs to be shifted to decode the message. Vigenère's clever idea was that we can set a codeword key of unknown length, the individual letters of which will then determine by how many positions we shift each successive character in the message to be encoded.

For example, let's say we agree on the key "ABC." Translating these letters into the number of shifts, we get:

A => 0; B => 1; C => 2.



PUBLIC DOMAIN, VIA WIKIMEDIA COMMONS

Fig. 3
Block encryption – the example photo is of Henryk Zygalski, one of the three Poznan cryptologists who broke the Enigma system

Let's say the message is: THEQUICKBROWNFOX. They key is reiterated to match the length of the message, so we use ABCABCABCABCABCA (which means: shift the first letter by zero positions, the next letter by one, the next by two, then repeat). The resulting encoded message is: TIGQVKCLDRPYNGQX.

By using a long enough codeword, we can make it very difficult to break such a cipher. When the length of the key is equal to the length of the message, so that each letter is shifted a different number of positions, we get a perfect cipher, called a *one-time pad*.

Breaking such codes is so difficult that in practice it is impossible without special methods. A complex device using a complex version of Vigenère's cipher, called the Enigma, was developed by the German military for use in World War II. An intricate system, encrypting virtually every letter with a different alphabet, made it nearly impenetrable. However, this code was first cracked in 1932 by Marian Rejewski, a graduate of the University of Poznań. Also instrumental to this breakthrough were Jerzy Różycki and Henryk Zygalski, Rejewski's colleagues at the Polish Cipher Bureau. They identified and exploited certain regularities in the Enigma's encryption patterns.

Block ciphers

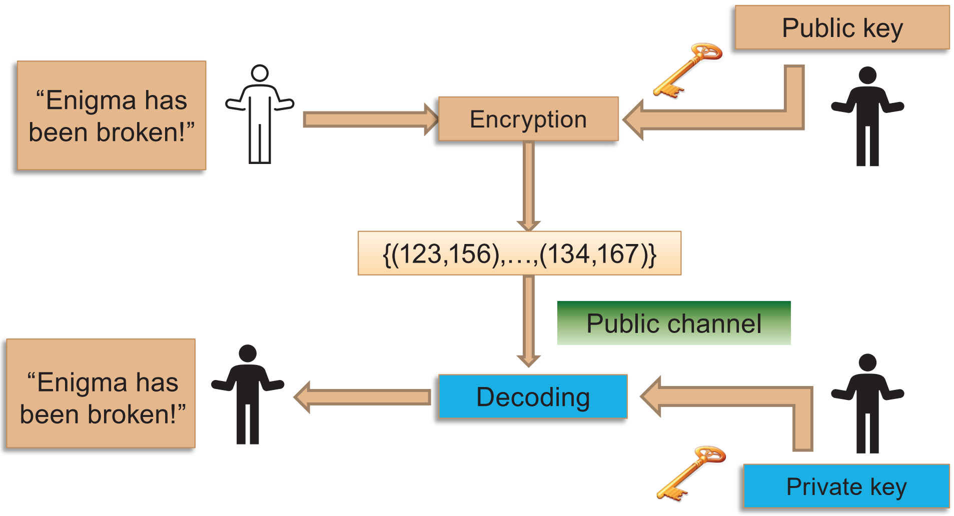
The era of the World Wars and post-war years saw the gradual transformation of encryption from the classical domain of linguistics into what we now call modern cryptography. A great leap forward came in the 1970s, when traditional character-based encryption was replaced by more sophisticated *block ciphers*.

Using a block cipher can be likened to shuffling a deck of cards. In each round, we perform operations that are seemingly trivial: confusion, masking with a key, diffusion (Fig. 3). Repeated many times, they give rise to tremendous complexity in the cipher. The Data Encryption Standard, invented in 1975, and its successor, the Advanced Encryption Standard from 2001, are currently the primary ciphers used for securely encoding very large messages. Practically all internet traffic is encrypted with the AES standard.

Interestingly, this cipher fundamentally relies on a single, computationally simple operation: calculating the inverse of an element in a finite field (specifically, a 256-element field). This gives us an improved Caesar cipher, ideal for encrypting a movie or other large datasets.

For ciphers to be used successfully, both the sender and receiver of the message must know the encryption key. In the mid-1970s, two solutions to this problem emerged in cryptography. The first idea involves generating a shared secret using the so-called Diffie-Hellman protocol. The second involves creating a procedure with two keys (Fig. 4): a public one, used only for encrypting messages, and a private one, used only for decoding them. We still need a procedure that will generate such a pair of keys and allow us to

Fig. 4
Cryptography with a public key



publicly share only the key marked as "public." This way, anyone can send us a secret, but no unauthorized person can read it without the private key. This idea was implemented in a concrete way by Ron Rivest, Adi Shamir and Leonard Adleman – their now widespread method is known as the *RSA algorithm*.

Forward into the future

Since the 1990s, the field of cryptography has increasingly become the domain of mathematicians specializing in numerical and algebraic theories. A notable advancement in recent years has been the transition from traditional exponentiation (raising a number to a power) to a more complex algebraic process known as *elliptic curve addition*. Elliptic curves are objects developed in the field of algebra and geometry, which have proved enormously useful in such diverse fields of science as high-energy physics, differential geometry, analysis, and number theory. The famous proof of the Fermat's Last Theorem put forward by Andrew Wiles in 1994 uses elliptic curves at crucial parts of the argument. Cryptographers were relatively slow to discover these mathematical objects, but when they did it was with great effect. Every aspect of our "online life" now uses elliptic curves to ensure a high level of security against password breaking.

In the 1980s, a certain threat to the security of the RSA algorithm and the Diffie-Hellman protocol emerged in the form of Peter Shor's factorization algorithm. Given a large quantum computer, this algorithm would easily break codes based on multiplication.

The increasingly robust development of quantum computing and quantum information theory has touched off another great leap forward by cryptographers dealing with RSA, elliptic curves, and factorization. Recent years have witnessed the birth of a completely new field, known as *post-quantum cryptography*. Currently, several encryption algorithms are competing to become the frontrunner, poised to replace all the existing protocols, which large quantum computers are expected to easily break in the future. The field is evolving rapidly and with high stakes. Among the dozens of candidates that were to the Post-Quantum Cryptography contest, announced in 2016 by the American National Institute of Standards and Technology, most have already been broken. The race continues among the winners of the fourth round of the contest, announced in 2022: CRYSTALS-Kyber (for generating a common secret), CRYSTALS-Dilithium, FALCON, and SPHINCS+ (algorithms for obtaining an electronic signature).

Another alternative is *quantum cryptography*: an extremely rapidly developing field of physics and quantum computing theory, working to construct laser-based systems for long-distance transmission of information that is highly secure (on the level of physical laws). The basic idea here involves generating a shared secret by utilizing the enigmatic phenomenon of quantum entanglement of particles. Polish scientists have significantly contributed to advancing this technology. Professor Artur Ekert, a theoretical physicist, was recently with the Milner Award for his contributions to the field.

Contemporary civilization is based on information and requires strong certifications of data transmission security. The security postulates are so demanding that to meet them, the complex and incredibly advanced mathematical apparatus of algebra, number theory, combinatorics, and statistics is marshalled into service. Therefore, it can be confidently said that mathematics has appeared practically everywhere thanks to the global Internet. It acts as a mysterious, "quiet and well-oiled" mechanism that, in a hidden way like in Umberto Eco's *Foucault's Pendulum*, governs our world and allows us to sleep peacefully as computational machines work hard to ensure our safety and prosperity. ■

RSA encryption

starts with selecting two very large prime numbers. We calculate their product, $N = pq$. Finding the values of p and q from the number N is an extremely difficult task (Fig. 5). A message sent using the RSA algorithm is a number, say m. Using the numbers p and q, we prepare a private and public key. We randomly choose a number e, which is coprime with *(p-1)(q-1)*. We calculate the number d, which has the property that *ed = 1 modulo (p-1)(q-1)*. We have obtained the private key (N, d) and the public key (N, e). A message can be safely transmitted by performing modular exponentiation: c = m^{e} modulo N. A third party without knowledge of the numbers p and q cannot recreate the message m. To decode the message, use: m = cd modulo N.

5

- We choose a large integer N. We establish two integers e and d, which provide reversible modulus operations ("wrapping around the clockface").
- RSA Encryption: we encode the message m as $c = m^{e}$.
- RSA Decoding: we decode the ciphertext c using c^{d}.
- Calculations are performed *modulo N* ("wrapping around the clockface").

RONALD L. RIVEST, CC BY-SA 4.0, VIA WIKIMEDIA COMMONS
THE ROYAL SOCIETY, CC BY-SA 3.0, VIA WIKIMEDIA COMMONS
LEN ADLMEN, CC BY-SA 3.0, VIA WIKIMEDIA COMMONS