FONDAZIONE BRUNO KESSLER
MAGAZINE

Cryptography: a millennia-long history

March 28, 2022

What trends for the future of Cybersecurity? An introductory lesson with Prof. Silvio Ranise, director of the Fondazione Bruno Kessler's Cybersecurity Center

What do the cult of the dead in ancient Egypt, the Spartan secret services in 900 BC, the 2400-year-old Indian Kamasutra and the Caesar cipher have in common?

Whether the purpose were to add mystery to the cult of the dead or to defend an “industrial” secret, or to communicate with generals or between lovers, **cryptography, for millennia, has allowed messages to be masked through puzzles and tricks that have evolved over the course of history up to today’s computer science**.

Silvio Ranise, director of the FBK **Cybersecurity** research center, briefly retraced this history to understand the complexity of current challenges and the application fields of cybersecurity techniques on a global scale, between latent threats to democracy and growing economic opportunities.

If in 100 BC, to understand a message written with Caesar’s cipher an average of a dozen attempts were enough; with current computers, we have managed to generate keys whose probability of being found is of the order of magnitude of 10 followed by 20 zeros, a hardly conceivable and almost unspeakable number.

In between, we have seen the **frequency analysis** suggested by Al Kindi in AD 850 to try to reduce the complexity of cipher attacks by using letter occurrence statistics as a clue to recognize cipher letters faster; later on, the father of modern cryptography, the Italian **Leon Battista Alberti**, a Renaissance genius who laid the foundations of modern cryptography and, finally, the recent developments in the 20th century, with the extraordinary feat of **Alan Turing**, who by decrypting the Nazis’ code Enigma is estimated to have helped bring forward the end of World War II by 2 years, saving 14 million lives.

Approaching the present day, we have moved on to the **Data Encryption Standard** (DES), developed in 1970 by IBM and adopted as a standard 7 years later until the end of 2000, with a key size of 56 bits, for a number of keys equal to 2 raised to the 56th power = 7*10 raised to the 16th power

Current cryptography has overtaken DES in conjunction with the growing computing power that has made the cost of the necessary computational capacity affordable (in 1999 about 250 thousand USD was enough). This led to the **Advanced Encryption Standard** at the end of 2001, generating approximately 1021 more keys than in the DES era.

In summary, the fundamental elements that characterize cryptography are the "**size of the keys**" and the **way in which they are distributed** to the participants. Modern techniques that combine symmetric (exploited for its efficiency) and public (used to define protocols for secure key management) cryptography are embedded into the internet network usage protocols (**HTTPS**) or are used in instant messaging systems (end to end encryption).

Such techniques protect the privacy of users, including those who exchange information to commit crimes. As a result, governments and law enforcement agencies have called for additional mechanisms that will allow them to control the content of messages exchanged by potential suspects. Unfortunately, this type of mechanism makes encryption useless as these vulnerabilities can be discovered independently even by malicious people who could exploit them for their own purposes.

To avoid this, Apple recently proposed an alternative technique called "client side scanning" which allows scanning of local resources to detect if there is something weird (e.g. child pornography images) and report it to the authorities. Despite the fact that this solution avoids adding vulnerabilities in ciphers, it presents other types of issues as, depending on the context in which it is added, it can involve risks both in ethical terms, discriminating and damaging democratic prerogatives, and in technical terms, presenting false positives.

The ending of this never-ending story is not only open but it's all in our hands. In her autobiography, entitled "In praise of imperfection" (Garzanti Editore, 1987), Nobel laureate **Rita Levi Montalcini** wrote: "The dizzying development of the constructive and destructive capacities of Homo Sapiens, in stark contrast to the sluggishness in the processing and manifestation of emotional faculties, to which today as in the past, the conduct of our actions is entrusted, is the primary cause of the dangers that threaten us."

PERMALINK

https://magazine.fbk.eu/en/news/cryptography-a-millennia-long-history/

TAGS

- #cryptography
- #cybersecurity
- #data
- #democracy
- #ethics
- #history
- #privacy
- #Technology

RELATED MEDIA

- FBK Cybersecurity research center : https://www.fbk.eu/en/cybersecurity/

AUTHORS

- Giancarlo Sciascia