# Safer, better, faster: addressing cryptography's big challenges

December 4 2008

(PhysOrg.com) -- Every time you use a credit card, access your bank account online or send secure email cryptography comes into play. But as computers become more powerful, network speeds increase and data storage grows, the current methods of protecting information are being challenged.

Once shrouded in secrecy, cryptography (using mathematical algorithms to secure, hide and authenticate data) has come out into the light in the current digital era. No longer restricted – in Western countries at least – by tight usage and export controls, cryptographers are now collaborating more extensively than ever before to create better algorithms and faster encryption methods to protect the vast volumes of data being generated by governments, businesses and citizens.

In many ways, European researchers are leading the way in addressing the big challenges facing the future of information and data security. "There are three big issues facing cryptographers," says Bart Preneel, a professor at Katholieke Universiteit Leuven in Belgium and president of the International Association for Cryptologic Research. "Cost, speed and long-term security."

The first two problems are closely interconnected, a consequence of the trend towards storing more information in more distributed systems, from the flash drives and smart cards in your pocket, to the computer in your home or the network at your office. Cost, in this sense, refers not only to the cost of hardware capable of robust encryption, but also the

energy cost of running cryptographic processes on increasingly tiny, low-power devices. Cryptographic programmes also need to be faster if they are to secure the vast amount of information now being stored.

## The 10 terabyte question

“In a few years we will have devices in our pockets with 10 terabytes of storage capacity – current methods are far too slow to encrypt that amount of data practically,” Preneel notes.

Time is also a problem in another sense. A lot of data being generated today will need to be kept secure for decades or even centuries to come, but history has shown that gains in computer processing power make it easier to crack cryptographic codes. Algorithms developed in the 1970s, for example, can now be readily broken by researchers.

“We may want to store medical information securely for a long time, not just for the duration of someone’s life, but in the case of DNA data for the lifetime of their children and grandchildren as well,” Preneel says.

Those challenges and others were addressed by an international network of researchers led by Preneel. With funding from the EU, the ECRYPT network of excellence brought together 32 leading research institutes, universities and companies to produce some of the most valuable contemporary research on cryptography, generating 10 percent of all papers and research articles in the information security field published worldwide over the last four years.

Structured into five core research areas, dubbed “virtual laboratories,” the researchers developed improved cryptographic algorithms, ciphers and hash functions, studied cryptographic protocols and implementation methods, and worked on more robust algorithms for digital watermarking.

Among their main achievements are eight new algorithms with the capacity to outperform AES, the Advanced Encryption Standard developed by two Belgian researchers in the 1990s and subsequently adopted by the US government to protect classified information. They also developed a new and improved method for creating cryptographic protocols based on game theory, and created lightweight cryptographic algorithms for use in low-power, low-computing-capacity devices such as smart cards and Radio Frequency Identification (RFID) tags.

Three competitions of the kind that sparked innovation in digital cryptography in the 1970s and 80s were also organised to find winning applications in the fields of stream ciphers, cryptographic software benchmarking and digital watermarking.

## Towards real-world applications

The researchers' work will all but certainly feed into commercial cryptographic applications over the coming years. A block cipher, for example, is due to be used on commercial RFID technology, while another application has been developed by Danish project partner Aarhus University for secure auctions in the agricultural sector.

Many of the researchers are continuing their work in a second project, ECRYPT II, which began in August 2008. Whereas ECRYPT received funding under the EU's Sixth Framework Programme for Research (FP6, 2002-2006), the follow-up initiative is being funded under FP7 (2007-2013). The new project will deepen research in core areas that were addressed more broadly by the first initiative.

"We know that our studies have been read by banks, businesses and governments around the world, but because we made the information publicly available we don't know how they are using it," Preneel says.

Cryptography has not, therefore, shed its veil of secrecy entirely.

*This is part one of a two-part series on ECRYPT.*
Part 2. Robust watermarking offers hope against digital piracy: www.physorg.com/news147701945.html

Provided by ICT Results