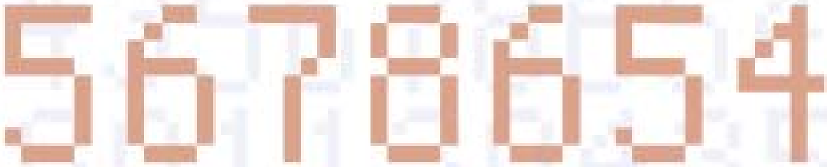
Sign of the times



Digital signatures are the next big step towards the paperless office. They depend on an extension of the encryption methods already used to secure email and other documents. Rupert Collins-White finds out how easy they are to falsify

Jens Franke and his colleagues crack numbers. Not just any numbers; they work in Bonn University and crack numbers that are the result of multiplying prime numbers. Last year Jens and his colleagues cracked RSA's 512bit cipher challenge. At the time of writing, they had almost finished breaking a 576bit key.

These big numbers (more than 150 digits long) make some of the most prominent encryption systems work. Popular encryption systems sold by RSA and Rabin owe their security to the 'integer factorisation problem' – very large numbers generated by multiplying large prime numbers that are extraordinarily hard to reduce back their primes unless you know what those primes are.

Cryptography is more complicated than that, but this mathematical peculiarity is the basis for the leading public key email encryption systems. In symmetric systems such as DES and AES the sender and recipient need to have the same key to lock and unlock the message.

In assymetric systems, such as RSA and Rabin, the sender uses a different encryption key to the receiver's decryption key. Mail is usually encrypted using DES or triple DES (3DES) and the encryption key itself secured using a second system, often an RSA or Rabin system.

Cracking good times

Both the US and UK governments are turning to AES for symmetric encryption – wise, given the propensity of drunken spooks for leaving laptops behind in London pubs.

But AES is unlikely to come to your office network anytime soon, particularly if you're using a system that's been reliable over a long period. Training and experience have taught network managers an almost Biblical fear of the unknown and they are not going to jump headfirst into something new. Many of us use Lotus Notes or Domino which employ RSA/DES mail encryption. Some experts believe that, for now, this type of email and signature encryption is relatively safe. Others claim that (at a key length many people use) RSA should be upgraded to 1,024 or even 2,048bit. And DES (and to a lesser extent 3DES) is obsolete and, worse, vulnerable.

Until recently the party line on encryption was that it would take supercomputers decades to crack it. But if the Bonn scientists are right, governments and some companies could crack encrypted information in less than a year for "under €3,000" – a remarkably conservative estimate considering the computing power available to an increasing number of organisations.

This calculation also assumes that the adversary has no knowledge other than the public key. The Bonn crackers do it the hard way with brute force attacks on keys. They don't use an encryption system's flaws to speed up the computation. Yet DES is well known for its flaws.

Organised crime and those with the right resources could probably crack this 'standard' crypto in far less time, and are almost certainly already doing so.

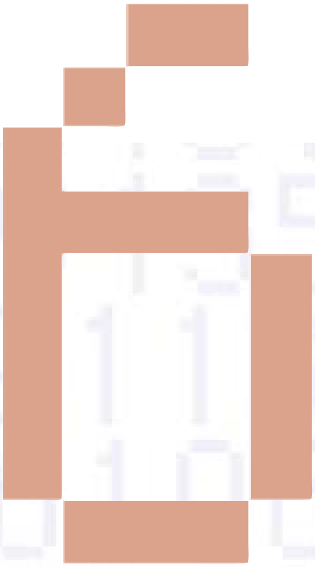
Level pegging

RSA held the US patent on the basics for sending encrypted mail. It has been telling the US government since the mid-90s that the level of encryption it was allowing out of the country was "vulnerable".

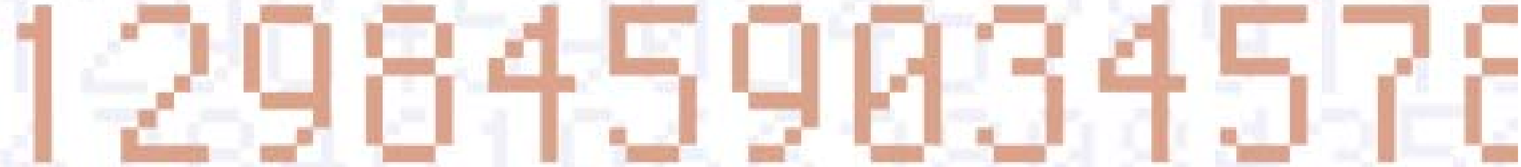
"RSA has been saying since 1995 to move away from 512bit keys," says RSA Labs director Burt Kaliski. "In the past export controls [from the US] played a part in the length of key paths." Kaliski suggests the known insecurity of 512bit (RSA) asymmetric and 40/56bit (DES) symmetric encryption and the fact these were the highest levels of security exportable from the US are "closely related".

Duncan Campbell, who wrote the EC's report on the Echelon spy network, agrees that the Bonn scientists' work shows the tools to crack RSA encryption are now in the open. But he also says it has been possible for more than a decade. "Attacks on robust, well-constructed ciphers have probably been easier for a lot longer [than is public now]," he says. "Encrypted information that was thought to have been safe for 20 years was probably safe for two months."

The government line, in both the US and here, has always been that export regulations for cryptographic



> “No one in the Russian mafia is going to want to spend 37 CPU years decrypting your personal emails just to find out what condition Auntie Gossie’s pacemaker is in”



products are set to prevent potential enemies, such as terrorists, organised crime and ‘rogue states’ getting hold of strong crypto.

Jim Dempsey, deputy director of the Center for Democracy and Technology in the US, confirms this: “It has been recognised for some time that 512 and 56 [bit lengths] were not secure under serious attacks, but the export regs were an attempt to limit what people could get.” But, he says, all that has changed.

“Now, what is safe and for what uses is up to the technology folks and the market to decide. The whole problem with the export controls was that they prevented that decision from being made on technical grounds.”

Winn Schwartau, an information warfare expert and director of security advisory firm Interpact agrees that, at bottom, crypto is safe despite the fact that it has been cracked at a high level. “Crypto is as strong as it is claimed, barring out-and-out errors, until the next brilliant guy comes along and proves everyone in the past was wrong. If that is what happened here [with Jens Franke’s ongoing work], the ramifications for speed, CPU horsepower and trust are certainly impressive,” he said.

Protecting what’s yours

Some experts say it’s often not the maths of security that is at fault but users who don’t protect their passwords and other vital security information. One said it’s almost unnecessary to crack keys as user error and ‘between the seams’ vulnerabilities were always more forthcoming.

This doesn’t matter a jot to the average PC punter. How long it takes to break a digital signature, potentially discovering a person’s private keys, comes down to how much time and cash you’re willing to throw at doing so. No one in the Russian mafia is going to want to spend 37 CPU years decrypting your personal emails just to find out what condition Auntie Gossie’s pacemaker is in.

Digital signatures work in roughly the same way as asymmetric key encryption in that a set of private keys is used to generate a one-time signature that can then be compared to a person’s public key and authenticated. It’s an ingenious system and one that can work wonders for online business. Digital signatures are a business and perhaps even a societal certainty. The trouble is, there’s no way to tell the difference between an authentic and a forged digital signature. If someone gets hold of the keys that make up your signature then, for all intents and purposes, they *are* you in the digital world.

The safest way to keep your private keys private is also one of the best ways to use digital signatures: on a card. Smartcard technology will probably become integral for nearly all our cards, no matter what they do. Smartcard makers claim that card technology is highly advanced and almost impossible to break into without ruining the card.

But last year Sergei Skorobogatov and Ross Anderson at University of Cambridge’s Computer Lab demonstrated how they could make a chip give up its secrets using a high-end microscope, a photo flashgun and a piece of aluminium foil. These attacks, while far more difficult now, prove that you never really know how vulnerable a seemingly secure system is.

Losing your identity

It’s clear that our everyday computer systems will become even more alarmingly advanced and powerful in the next decade. And if you don’t even need high-end processing to circumvent a smartcard, who knows how easy it will become to steal your identity?”

“The RSA key length may indeed be a problem for keys that are used to produce signatures that have a long-term validity [such as legal contracts],” says Joan Daemen, one of the co-inventors of Rijndael (later AES).

“However, there are many more problems in using smartcards for electronic signatures that currently have no solution. The most important ones are related to key management, registration authorities and assuring that the smartcard actually signs what the cardholder wants his card to sign.

“In my opinion, one should not use smartcard-generated signatures alone to protect legal contracts. However, they can help to replace (or complement) handwritten signatures”, says Daemen.

So we’re back to blowing dandelions again. They’re safe. They’re not safe. They’re safe. They’re not safe. They’re safe… for now. ☒