Scott Vanstone on current public key sizes *page 2*

William Tutte: a tribute *page 3*

New attack on RSA-based SSL *page 4*

Attack on NTRU and other crypto news *page 6*

Certicom's Bulletin of Security and Cryptography

CØDE&CIPHER

The premier issue of Code and Cipher is dedicated to the memory of William Thomas Tutte (1917-2002), distinguished Professor Emeritus and Honorary Director of the Centre for Applied Cryptographic Research at the University of Waterloo and one of the most influential figures in combinatorics.

The Next Generation of Cryptography

Public Key Sizes for AES

With recent world events, security has become an important issue with decision makers in both business and government. This focus on security is evident in the digital world where protecting sensitive information is mission critical. Exponential improvements in computing power over the last 20 years have forced cryptographers to design new algorithms that can stay secure for another 20 years.

The 56-bit Data Encryption Standard (DES) has now been replaced with the Advanced Encryption Standard (AES), which provides at least 128 bits of security and a scaleable key size that solves the demand for stronger security. However, a stronger algorithm like AES demands equivalent security for the accompanying digital signatures and key exchanges. Otherwise, AES can be compromised through the weaker security of public-key cryptography.

According to the National Institute of Standards and Technology (NIST), keys for symmetric ciphers such as AES must be matched in strength by public key algorithms such as RSA and Elliptic Curve Cryptography (ECC). For example a 128-bit AES key demands a 3072-bit RSA key while 256-bit AES demands an RSA key size of 15,360 bits for equivalent security. Clearly, 15,360 bits would bring almost any system to its knees since key size is directly related to computing resources.

Fortunately, ECC scales linearly with AES and maintains relatively compact key sizes at all security levels. ECC keys by comparison are only 512 bits for 256-bit AES and therefore do not hinder performance. AES, used in conjunction with ECC, allows for high security solutions that do not impact performance even on constrained devices such as PDAs and cell phones where computing power is only a fraction of what's available on a desktop.

The Advanced Encryption Standard

AES was selected through a public process that was in fact a contest conducted by the NIST, the US Government's official standards organization. Fifteen candidates submitted symmetric encryption algorithms that met NIST requirements. Five of these contestants made it into the AES finals. The five finalists were all regarded to have similar security, but the submission from Rijndael

continues on page 5

Welcome to Code and Cipher

Code and Cipher, published quarterly by Certicom Corp., is an educational newsletter that covers the security and cryptography industry. In each issue we will examine security issues and cryptography trends in an objective manner. We welcome your thoughts, opinions and comments on anything that affects the industry. Please send your feedback on this issue and what you'd like to see in upcoming ones to: codeandcipher@certicom.com.

Crypto Column by Dr. Scott Vanstone

Are Current Public Key Sizes Good Enough?

There has been much discussion lately about RSA public key sizes for a number of reasons. Those who are reluctant to migrate from 1024-bit RSA to the larger keys sizes defend these RSA keys by arguing that they are strong enough for the foreseeable future and that they don't want to increase costs. These arguments are being called into question.

Many security deployments implement the 1024-bit RSA for key transport because it's relatively easy to get an X.509 digital certificate that uses 1024-bit RSA from a number of commercial certificate providers. This is a very dangerous approach because the security of the public key system must be matched with the symmetric cipher used. NIST mandates it and it's only common sense. We know that 1024-bit RSA does not match the 128-bit security level now used for symmetric ciphers as the two recent examples outlined below demonstrate.

First, research published this past February by Adi Shamir, the "S" in RSA, raises new concerns about the security of 1024-bit RSA. His paper describes a new hardware implementation for factoring that makes it 3 to 4 orders more cost-effective than previous designs. He estimates the factoring for 512-bit RSA can be completed in 10 minutes by a $10K device and 1024-bit RSA in less than 1 year with a $10M device. It sounds like a lot of money, but since every secure e-commerce server on the planet uses 1024-bit RSA (in SSL/TLS), the investment may be a good one for certain parties.

The second is highlighted by Microsoft's concern with RSA key size when they built the Xbox. They chose to install a 2,048-bit RSA key to prevent the user from running executables that have not been authorized by Microsoft. Despite little chance of success, a group of hackers started the Neo Project that uses distributed computing techniques (similar to the Seti@Home project) to recover the secret key.

The Neo Project software is now running on thousands of idle PC resources to try to guess the 2,048-bit encryption key used by the Xbox, a brute force approach that will likely never yield the result. While a brute force attack may be fun to watch, Shamir is on the right track by using mathematics to improve the likelihood of recovering the key.

The bottom line is that implementers should not be complacent with 1024-bit RSA as it may be practically broken sooner than you think. Security systems need to be designed to have a reasonable lifetime in the field.

We know many organizations understand this when looking at symmetric ciphers as they are moving from 3DES to AES, even if they only moved from DES a couple of years ago. However, when making this move to 128-bit AES, you need to use a matching public key scheme that demands 3072-bit RSA or 256-bit ECC. As you can see in this issue, there are tradeoffs in efficiency when making this decision. The important thing to remember is to not compromise the security of the system and to address these performance issues.

A Tribute to William Thomas Tutte (1917-2002)

Mathematician and Cryptographer

Although not a household name, William Thomas Tutte was a world-renowned mathematician and one of the most influential figures in combinatorics. He was instrumental in developing the reputation of the University of Waterloo and the Faculty of Mathematics. But arguably Tutte's best work, not known until recently, was as a master codebreaker at Bletchley Park, the now-legendary organization of code-breakers of Britain.

At Bletchley Park, Tutte managed to break Fish, a series of German military codes for encrypting communications. Termed "the greatest intellectual feat of the whole war," the work on Fish led to the development of Colossus, "the world's first electronic computer," in which Tutte also played a key role.

There is widespread knowledge of the successes they had deciphering the codes produced by the machines called Enigma. Broadly speaking, what Alan Turing did for Enigma, Tutte did for cracking the Lorenz cipher, codenamed "Fish" by the British.

Tutte's work at Bletchley Park breaking German codes has been hailed as "the greatest intellectual feat of the whole war."

The son of a gardener, William Tutte was born at Newmarket, England, where he went to local schools. At 18, he was a natural candidate for a place at Trinity College, Cambridge, where he studied chemistry from 1935, before moving on to postgraduate research. It was there that he formed a particularly close bond with three fellow members of the Trinity Mathematical Society. The group collaborated on the problem of "squaring the square" – dividing a square into unequal smaller squares – and in 1940 published a paper that described their solution; Tutte believed that it was as a result of this work that he was asked to go to Bletchley Park.

Within months of going to Bletchley, Tutte had achieved a breakthrough, thanks to a security blunder by a German operator. Two different texts of the same lengthy message were intercepted, the one an apparently corrected or tidied-up version of the other. But each had the same opening letters, the identifying "indicator" to the recipient, and the same "padding", or throwaway letters, routinely added to all messages to confuse eavesdroppers and cryptanalysts.

Using these two messages, after four months' toil, in which he worked from the messages alone and wrote out vast sequences by hand, Tutte deduced the structure of the machines. In a sequence of brilliant observations, he deduced that there was in the Lorenz machine a wheel of 41 sprockets, and another with 31. He went on, with others at Bletchley, to calculate that there were 12 wheels, and also determined the structure of their interconnection. He had worked out the entire machine without ever having seen one.

Tutte was then involved in creating algorithms to break the codes and to decipher the messages that the Fish machines produced. The deciphering continued into 1943, but then the Germans took precautions to make decoding more difficult. The algorithms developed by Tutte and his colleagues, Max Newman and Ralph Tester, could be carried out only by machine.

This prompted the development by post office engineers, working with Bletchley, of the world's first electronic computer, the Colossus – a vast machine with radio valves and a tiny fraction of the capacity of a modern laptop. With the aid of Colossus, and using Tutte's algorithms to break the Lorenz codes, vital intelligence was obtained about Hitler's intentions in the run up to D-Day in 1944.

After this unique intellectual feat and contribution to the war effort, Tutte modestly returned to academic life and mathematical studies at Cambridge. Upon receiving his PhD, Tutte came to Canada to join the faculty of the University of Toronto. In his 14 years there, he rose to world pre-eminence in the emerging field of combinatorics.

In 1962, Tutte joined the faculty of the University of Waterloo (UW) and made a major contribution towards its identity and reputation. His presence was a magnet for combinatorialists from throughout the world. It was not only the recognized stars of the field that came to UW, but those who were destined for future prominence. Tutte was named Honorary Director of the Center for Applied Cryptographic Research in 1998.

Tutte's accomplishments have been recognized through many significant honours and prizes. He was the recipient of a prestigious Izaak Walton Killam Memorial Prize in 1982 as "one of the most respected mathematicians in the world today." Before receiving the Order of Canada, he was elected to the Royal Society of Canada and then to the Royal Society of London.

Tutte passed away on May 2, 2002. As we approach the first anniversary of his death, many will remember his great contributions to the fields of mathematics and cryptography while those that knew him will remember him as a great colleague and a true gentleman. He will be truly missed.

At the opening ceremony for the
Centre for Applied Cryptographic Reseach at the University of Waterloo
(June 19, 1998) Tutte gave a lecture titled "Fish and I".
For a copy of his speech, visit
www.cacr.math.uwaterloo.ca/techreports/1998/corr98-39.pdf

New Attack on RSA-based SSL/TLS Protocol

Affects Two-Thirds of all Web Servers

As the number of digital transactions increases explosively each year, more and more people place their trust in the security that underlies e-commerce. As we have seen before, only years of study can ensure that the underlying cryptography is strong. However, even trusted protocols such as SSL can have weaknesses that are exposed after many years of use.

Czech cryptographers Klima, Pokorny and Rosa have discoverd such an attack on the RSA-based SSL/TLS protocol and made it publicly available March 14, 2003 on the International Association of Cryptologic Research ePrint server. (http://eprint.iacr.org/2003/052/)

In fact, practical tests showed that two-thirds of randomly chosen SSL/TLS web servers were vulnerable.

Summary of the Attack

The attack extends a famous attack of Bleichenbacher from the Advances in Cryptology 1998 conference. Bleichenbacher's attack exploits features in PKCS #1 version 1.5 padding used for RSA encryption, and in particular how this PKCS #1 version 1.5 padding was used in the SSL/TLS protocol.

Klima, Pokorny and Rosa's attack is more specific to SSL/TLS protocol than Bleichenbacher's attack, but similar in its underlying mathematics. It exploits alert messages sent during the SSL/TLS protocol resulting from incorrect lengths of the plaintext or from incorrect SSL/TLS version numbers contained in the plaintext.

Each such alert message can be used to leak, according to Klima, Pokorny and Rosa, a small amount of information about the master key used for a previous SSL/TLS. Eventually this leaked information, the authors claim, can be accumulated together and the master key of a previous SSL/TLS session can be recovered, allowing the adversary to decrypt all the messages protected during that session.

Klima, Pokorny and Rosa examined several SSL/TLS servers for potential vulnerability to their attack by examining the frequency with which the dangerous alerts were issued. They found that several servers with OpenSSL, which is used in approximately 50% of all e-commerce web servers, issued leaky alerts at considerable rates. From these rates, the authors estimated that if their attack was implemented, it could compromise a previous SSL/TLS session by bombarding an SSL/TLS server with specially chosen RSA ciphertexts for 56 hours continuously.

Find a copy of Klima, Pokorny and Rosa's paper *Attacking RSA-based Sessions in SSL/TLS* at http://eprint.iacr.org/2003/052/

Assessment of the Attack

The damage of the attack is specific to the RSA algorithm, and the PKCS #1 version 1.5 padding in particular. Furthermore, it is limited to the SSL/TLS protocol, unlike Bleichenbacher's original attack that affected more general uses of RSA with PKCS #1 version 1.5 padding.

The viability of the attack is limited by the need to bombard an SSL/TLS server with copious amounts of invalid RSA ciphertexts. In practice, an SSL/TLS server might not allow such a large amount of invalid ciphertexts. Nevertheless, such limitations are inappropriate countermeasures for such an attack because of their lack of cryptographic robustness.

Despite the limitations above, the sheer ubiquity of SSL/TLS using RSA with PKCS #1 version 1.5 compensates to make the impact of the Klima, Pokorny and Rosa attack potentially very harmful. As well, Klima, Pokorny and Rosa's attack might extend to other forms of RSA padding, such as OAEP (Optimal Asymmetric Encryption Padding), by analogy to Manger's extension of Bleichenbacher's attack.

Interestingly, Klima, Pokorny and Rosa's attack does not apply to SSL/TLS using ECC because it uses key agreement rather than key transport to transmit the "pre-master secret". In particular, this means that the pre-master secret is not conveyed in a plaintext, but rather more indirectly by calculations done on both the client side and the server side. As a result, there is no plaintext used to transmit the pre-master secret, which is the crux of the Klima, Pokorny and Rosa attack. Therefore, no version number and no length in the plaintext need checking so the problematic alert messages used by the attack are not generated when using ECC.

Reactions to the Attack

Klima, Pokorny and Rosa suggest a countermeasure that they deem optimal. In their countermeasure, a SSL/TLS server, instead of issuing an alert immediately upon discovery of an invalid length or version, replaces the offending pre-master secret by a random one, and proceeds as though everything was fine.

The OpenSSL group issued a patch that aimed to prevent Klima, Pokorny and Rosa's attack. The patch essentially implemented the countermeasure recommended by Klima, Pokorny and Rosa.

Only time will tell if this change prevents exposing the protocol to yet other attacks, such as those based on timing analysis.

Security (bits)	Symmetric encryption algorithm	Hash algorithm	Minimum Size of Public Keys (bits)		
			DSA/DH	RSA	ECC
80	–	SHA-1	1024	1024	160
112	3DES	–	2048	2048	224
128	AES-128	SHA-256	3072	3072	256
192	AES-192	SHA-384	7680	7680	384
256	AES-256	SHA-512	15360	15360	512

Table 1: NIST Guidelines for the equivalent strengths of various cryptographic algorithms.

continued from page 1

The Next Generation of Cryptography

was selected to become AES as it offered the best performance across all architectures.

In fact, NIST now specifies AES in the document Federal Information Processing Standard (FIPS) 197 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf), as the new standard for symmetric encryption. AES succeeds DES and Triple-DES, which are symmetric encryption algorithms that provide 56 and 112 bits of security, respectively, that were formerly approved for use by US government organizations.

To date, AES remains the only symmetric encryption algorithm providing at least 128 bits of security that is approved for use by US government organizations to protect sensitive, unclassified information (http://csrc.nist.gov/encryption/aes/frn-fips197.pdf). AES comes in three security strengths: 128 bits, 192 bits and 256 bits. The 128-bit strength should provide at least 30 years of protection (http://csrc.nist.gov/policies/ombencryption-guidance.pdf). The higher strengths are available for even greater protection.

Surprisingly, not only does AES provide more security than 3DES, it also delivers better performance. Better performance and better security make AES a highly attractive alternative to 3DES and a good choice for symmetric encryption algorithm going forward.

Public Key Systems for AES

Symmetric-key cryptography algorithms are very fast but not that versatile. Key management with only symmetric-key algorithms is very difficult and non-repudiation is unattainable. Asymmetric-key cryptography, also known as public-key cryptography, resolves these problems. Public-key cryptography also provides digital signatures for non-repudiation and key agreement techniques that greatly simplify key management.

Today, there are three types of public-key cryptographic systems that can be considered secure and efficient. These systems, classified according to the mathematical problem on which they are based, are: Integer Factorization systems (of which RSA is the best known example), Discrete Logarithm systems (such as the US Government's DSA), and the Elliptic Curve Cryptosystem. The two major benchmarks when comparing these systems are security and efficiency.

As shown in Table 1, at all levels of security including 128 bits, ECC has smaller public key sizes than both RSA and DSA/DH. Because of its smaller key size, ECC outperforms both RSA and DSA/DH for most routine operations while offering comparable levels of security. The reason is that ECC provides greater efficiency in terms of computational overheads, key sizes and bandwidth. In implementations, these savings mean higher speeds, lower power consumption, and code size reductions. The gap between systems grows as the key sizes increase which is especially relevant to implementations of AES.

The performance advantage of ECC for AES would be all for naught if there was not widespread employment of the system in standards. ECC is a public-key cryptography technique approved for digital signatures used by the US Government, as specified by NIST in its publication FIPS 186-2 (http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf). Organizations such as ANSI, IETF, ISO and IEEE have also endorsed ECC as a public-key cryptography standard.

Conclusions

The Advanced Encryption Standard has set a new bar for secure systems for years to come. The security of the public-key system must match AES. The NIST guidelines demonstrate that ECC's key sizes scale perfectly with AES while the other systems clearly do not. The future of Internet security standards such as SSL/TLS, S/MIME and IKE/IPSec depends on public key systems that match the security of AES and offer performance that does not impact the user. ECC delivers the highest strength-per-bit of any public key cryptography known today.

For more background on public-key cryptography systems, read the Certicom whitepaper: *Current Pu blic-Key Cryptographic Systems* found at http://www.certicom.com/resources/download/EccWhite2.pdf

Crypto News

ATTACK ON THE NTRU ENCRYPTION SCHEME

In January, John Proos, a PhD student at the University of Waterloo, published a research paper entitled "Imperfect Decryption and an Attack on the NTRU Encryption Scheme." Proos found that given an NTRU public key, there exist ciphertexts that can be validly created using the public key but can't be decrypted using the private key. The valid ciphertexts, that an NTRU secret key will not correctly decipher determine, up to a cyclic shift, the secret key. In this paper, Proos explains attacks based on this property against the NTRU primitive and many of the suggested NTRU padding schemes. These attacks are quite practical, taking a few minutes on a single PC. Visit http://www.cacr.math.uwaterloo.ca/techreports/2003/corr2003-01.pdf for a copy of Proos' paper.

FACTORING FOR 1024-BIT RSA KEYS

In February, Adi Shamir and Eran Tromer published "Factoring Large Numbers with the TWIRL Device", which raises some concerns about the security of 1024-bit RSA keys. The security of RSA depends on the difficulty of factoring large integers. In 1999, a large distributed computation involving hundreds of workstations working for many months managed to factor a 512-bit RSA key, but 1024-bit keys were believed to be safe for the next 15-20 years. This paper describes a new hardware implementation, 3-4 orders of magnitude more cost effective than the best previously published designs, and suggests that factoring for 1024-bit RSA keys can be completed in less than a year by a $10M device. Visit http://www.wisdom.weizmann.ac.il/~tromer/papers/twirl.pdf to find a copy of the paper.

VALIDATION FOR ELLIPTIC CURVE PUBLIC KEYS

In January, Adrian Antipa, Daniel Brown, Alfred Menezes, Rene Struik and Scott Vanstone published "Validation of Elliptic Curve Public Keys" in Conference Proceedings of Public Key Cryptography – PKC 2003. In this work, they show that an implementation of elliptic curve cryptography (ECC) must be extremely careful to validate elliptic curve public keys, otherwise private keys could be compromised very easily. A few standards, including IEEE 1363-2000 neither require public key validation nor provide adequate warning, while other standards, including ANSI X9.63 require public key validation. Visit http://grouper.ieee.org/groups/1363/WorkingGroup/presentations/Jan03.html to see the presentation.

UPCOMING EVENTS

THE 7TH WORKSHOP ON ELLIPTIC CURVE CRYPTOGRAPHY (ECC 2003)

University of Waterloo
Waterloo, Ontario, Canada
August 11, 12 & 13 2003

For more information visit:
http://www.cacr.math.uwaterloo.ca/conferences/2003/ecc2003/announcement.html

BOOK RELEASE

Guide to Elliptic Curve Cryptography

by Darrel Hankerson, Alfred Menezes and Scott Vanstone

Coming in Fall 2003 from Springer-Verlag.

Code and Cipher is published quarterly by Certicom Corp.

5520 Explorer Drive, 4th Floor
Mississauga, Ontario, L4W 5L1
Canada

T (905) 507-4220
F (905) 507-4230
E codeandcipher@certicom.com

certicom™