Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: wsp@cnp-wireless.com Vol. 3, No. 8. September, 2001

Rijndael Revealed

Greg Rose, QUALCOMM Australia

Rijndael is the newly selected Advanced Encryption Standard algorithm. In this article, we look at how it got there and how it works.

A Brief History of DES

- Back in the early 1970s, the use of encryption was largely restricted to military applications, and there were very few resources available in the commercial world. However, the financial community needed security to allow inter-bank and foreign exchange communications, and the U.S. government wanted a cipher that could be used for non-classified applications.
- So, the U.S. National Bureau of Standards (now NIST), went looking for a Data Encryption Standard (DES) algorithm, and it found one at IBM. DES (Technically, DES is a standard, not an algorithm, and the algorithm it defines is actually DEA, but we'll stick with the common usage and call the algorithm DES) was designed by Horst Feistel, Don Coppersmith, and a number of others at IBM's T.J. Watson Research Center, with a little bit of assistance from the NSA. It was a development of an earlier cipher called Lucifer. FIPS 46 was published in 1974.
- The new algorithm was criticized immediately, for two reasons. DES' key length, at 56 bits, was already thought to be too short; Lucifer had 128 bit keys, and the few "public" cryptographers at the time saw no reason why the new algorithm shouldn't do the same. Also, the algorithm had "S-boxes," short for "substitution boxes," but no criteria had been given for the design of these non-linear lookup tables; there was widespread paranoia that the secret design somehow held cryptographic backdoors that enabled those "in the know" (that is, the NSA) to break it easily. When Biham and Shamir independently discovered a technique called Differential Cryptanalysis in 1989, it became clear that this secrecy was because DES was stronger than the public knew, not weaker. However, revealing this fact would also have revealed a powerful and top-secret cryptanalytic attack.
- Of the two problems, though, the short key was insurmountable. FIP Standards are time-limited, and when it was time to review DES, it was renewed for five years in 1989, when most cryptographers thought it shouldn't have been. Michael Wiener published the design of a machine, which, if built, would be able to break DES by brute force. In 1994, FIPS 86 was again renewed, introducing "triple DES" as a patch to keep the aging DES alive. RSA Data Security Inc. offered a cash prize to the first break of DES, which was done by a cooperative effort of many

About Wireless Security Perspectives

Price

The basic subscription price for *Wireless Security Perspectives* is $300 for one year (12 issues) for delivery by emailed PDF file or by first class mail within the US or Canada. International subscriptions are US$350 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees to allow more readers.

We provide discounts to educational institutions and small businesses (less than 10 employees).

Back issues are available individually, or in bulk at reduced prices.

Delivery is by first class mail or by email (Acrobat PDF file).

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due…

October 15th, 2001.

Future Topics

Wireless Packet Data Security • IP Security • Public Keys & Wireless • IP Mobility Security • Security Issues in Ad hoc Wireless Networks • Electronic Signatures in Wireless • Latest in Watermarking

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary, Alberta T2N 3W1, Canada. **Phone**: 1-800-633-5514 (+1-403-274-4749) **Fax**: +1-403-289-6658 **Email**: cnpsales@cnp-wireless.com **Web**: www.cnp-wireless.com/wsp.html. **Subscriptions**: $300 for delivery in the USA or Canada, US$350 elsewhere. **Payment**: accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery**: Email or 1st class mail. **Back Issues**: Available individually for $35 in the US and Canada and US$40 elsewhere, or in bulk at reduced rates. **Discounts**: Educational and small business discount: 25% off any order. **Copies**: Each subscriber is licensed to make up to 10 copies of each issue or back issue. Call for rates to allow more copies.

Technical Editor: Les Owens.
Article Sourcing: Betsy Harter.
Production: Doug Scofield.
Distribution: Debbie Brandelli.
Marketing: Muneerah Vasanji.
Accounts: Evelyn Goreham.
Publisher: David Crowe.

Upcoming Fraud and Security Events

The following are some upcoming fraud and security conferences and events that may be of interest to wireless security and network security practitioners.

Mobile Internet 2001
19-22 September, 2001
CNIT Center
Paris
www.mobileinternetexpo.com

SANS Network Security 2001 7th Annual Conference on Securing Networks and Systems
15-22 October, 2001
Town & Country Hotel and Convention Center
San Diego
www.sans.org/NS2001/NS2001.htm

IPSec 2001 Global Summit (Third Annual)
23-26 October, 2001
Paris
www.upperside.fr/ipsec2001/ipsec01intro.htm

The World E-Police Summit
Demonstrating the Strategic Business Benefits of E-Policing Technology
24-25 October, 2001
Holiday Inn, Victoria
London, UK
www.iqpc.com/cgi-bin/templates/9998409867635192871080002/genevent.html?event=1811&topic=

The CSI 28th Annual Computer Security Conference and Exhibition
29-31 October, 2001
Marriot Wardman Park Hotel
Washington, DC
www.gocsi.com/28th_annual

Federal Information Assurance Conference
31 October - 1 November, 2001
The Inn and Conference Center
College Park, MD
www.fbcinc.com/FIAC

National Space INFOSEC Symposium
6-8 November 2001
The Aerospace Corporation
El Segundo, CA
www.iaevents.com/NEW_ElSegundo/NewInfo.html

Securing New Ground - 6th Annual Conference
The New World of Security
7-8 November 2001
Roosevelt Hotel
New York City
www.securingnewground.com/default.asp

Ensuring End-to-End Security for Wireless Networking
29-30 November 2001
Washington Court Hotel
Washington, DC
www.iirusa.com/security/index.cfm

Internet-connected workstations. In 1998, though, DES was truly demolished, after the Electronic Frontier Foundation spent $250,000 to build Deep Crack, which broke DES in 56 hours, for an estimated amortized cost of about $1,000. Clearly this cipher could no longer protect billion-dollar transactions.

- So, in 1998, the U.S. National Institute of Standards and Technology (NIST) announced a search for the Advanced Encryption Standard to replace DES.

The Advanced Encryption Standard Process

The search for AES would take about three years. First, algorithms were solicited from around the world to meet specified design criteria for block size key lengths and intellectual property restrictions (they had to be free for use, if selected). Then, the 15 candidates meeting the submission criteria were presented at the first AES conference (three were found flawed either at the conference or before it), and a year of public study was allowed. Of the proposals, five then became "finalists": MARS from IBM; RC6 from RSA Data Security; Rijndael by Joan Daemen and Vincent Rijmen of Belgium; Serpent by a multinational team of Ross Anderson, Eli Biham, and Lars Knudsen; and Twofish, principally from Counterpane. After another year of study, Rijndael was selected to be the Advanced Encryption Standard algorithm.

The AES specifies a block cipher with block length (that is, the unit of a single encryption operation) of 128 bits, and key lengths of 128, 192 and 256 bits. Most of the algorithms submitted would support other key sizes and/or block sizes. NIST said there were no known security problems with any of the finalists.

And the winner is: Rijndael

It's my opinion that Rijndael was an obvious winner, so long as only technological reasons for selection were considered. Under special conditions, one of the other candidates might just outperform it (different candidates for different conditions), but across the board, it was the fastest and simplest algorithm. Its mathematical structure was both easy to implement and easy to analyze. Rijndael also has a property called "key agility" that enables it to rapidly switch between keys, which is very important for applications like IPSec. At the final AES conference, three of the teams chose Rijndael as their preferred winner if their own algorithm couldn't win (Rijmen chose Serpent, and the IBM team declined to answer the question).

Rijndael actually supports longer blocks (multiples of 64 bits) and other key lengths (multiples of 32 bits), but the FIPS stays with the original specification. Some of the parameters of Rijndael differ according to the number of bits in the key or block, but for this article, I will ignore this, talking only about the 128/128 bit version as used by TIA and 3GPP.

Rijndael was based on an earlier design by the same authors, called Square (the reason for the name will become obvious below). As it turns out, Rijndael is Flemish (Belgian) for "Rhine valley,"

and the authors like wine from that region. When it was suggested that the name was too hard to pronounce (it is something like saying "rain doll" while coughing), the authors pointed out that there was a Flemish word consisting entirely of vowels. A Canadian cryptographer suggested "Bob", but this was rebuffed.

Rijndael has quickly been adopted for many applications. A number of standards had been drafted with "AES goes here," and it appears in places such as TLS, IPSec, TIA's Enhanced Privacy algorithm and 3GPP's MILENAGE (recommended for Authenticated Key Agreement).

How Rijndael works

Rijndael is, in the cryptic language of cryptographers, an iterated substitution-permutation network cipher. "Iterated" just means there are a number of "rounds" of operations, and each round is essentially the same. Rijndael has 10 rounds. An "S-P network" is a cipher where every round changes the entire data block by substituting values by other values and then moving the bits around in the block (permuting them). Each round combines information derived from the key and the (permuted) data. Each round can be reversed by reversing the effect of the key material, unshuffling the bits and doing the reverse substitution, so undoing the rounds in reverse order performs decryption.

Rijndael makes use of alternating views of the data, treating the 128-bit block either as 16 bytes, or as four 32-bit words (most significant byte first). The bytes are thought of as being arranged in a square, and the columns of the square form the words (from now on, when I say words, I mean these 32-bit words formed from 4 bytes).

The real elegance of Rijndael shows up in the fact that all of the operations mentioned below are implemented with exclusive-or (XOR) or by looking up tables, and when you're going to use the result of one table lookup to look up another table, the tables can be combined for efficiency. An efficient implementation can do as little as 160 XOR operations and 160 table lookups (in 256-entry tables) to encrypt or decrypt an entire block. To explain what's happening "under the covers," though, I'll ignore these optimizations, talking only about the basic operations.

Key expansion

Before you actually encrypt something, and if efficiency is a consideration, you first do an operation called "key scheduling," which expands the secret key into subkeys (and perhaps key-dependent tables) ready to be used by the rounds of the algorithm. Rijndael needs eleven (11) subkeys – each of 16 bytes – from the original key. Treating the key as words, you start to fill an array with new words by XORing the previous word and the one four words before. There's a small catch, though. Every fourth word is modified through the ByteSub transformation mentioned below. This means the subkeys are all tied together, but they are related in non-linear ways that are hard to solve.

Overall structure

The rounds themselves are fairly simple, consisting of just four steps:

- Byte substitution
- Shift rows
- Mix columns
- XOR subkey

Before running the rounds, the data block and the first subkey are XORed. Then there are 10 rounds of the same operations, except that in the last round the last mix-column operation is not done. The first and final XOR operations are called "whitening"; these make it difficult to mount certain kinds of attack.

Byte substitution and the S-box

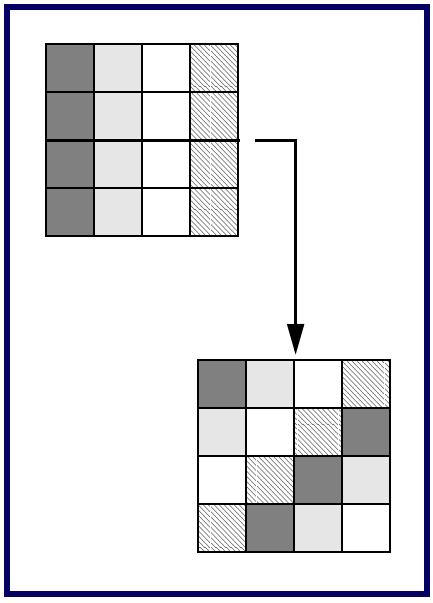
Rijndael has a single table, called the S-box – after DES – which implements a highly non-linear permutation. Given an 8-bit value, looking up that entry in the S-box returns a different 8-bit value, in a way that lets the operation be reversed for decryption. But the table is defined in a way that there is no simple formula describing the change in the data byte. There aren't even simple formulas that are "close" or "correct most of the time" – that's what "highly non-linear" means.

The byte substitution operation is simply replacing each byte of the data block by the corresponding table value. It's also used in the key scheduling operation.

Shift rows

This one really is best shown graphically. Figure 1 demonstrates why Square was called what it was.

Figure 1: Square



As you can see, each of the rows is shifted around the square shape, which doesn't by itself do very much. What it does, though, is put the bytes in position ready for the next operation.

Mix columns

This operation applies a mathematical operation to each of the four columns, treating the bytes as coefficients of a polynomial and multiplying it by a constant polynomial, modulo yet another polynomial. This operation is especially complicated when you realize that the coefficients are also polynomials, with binary coefficients. But don't panic. It's all meaningful, mathematically speaking,

and the complication is exactly what is needed for encryption. This has the effect of spreading out each byte, so that any change in it affects the whole word.

XOR subkey

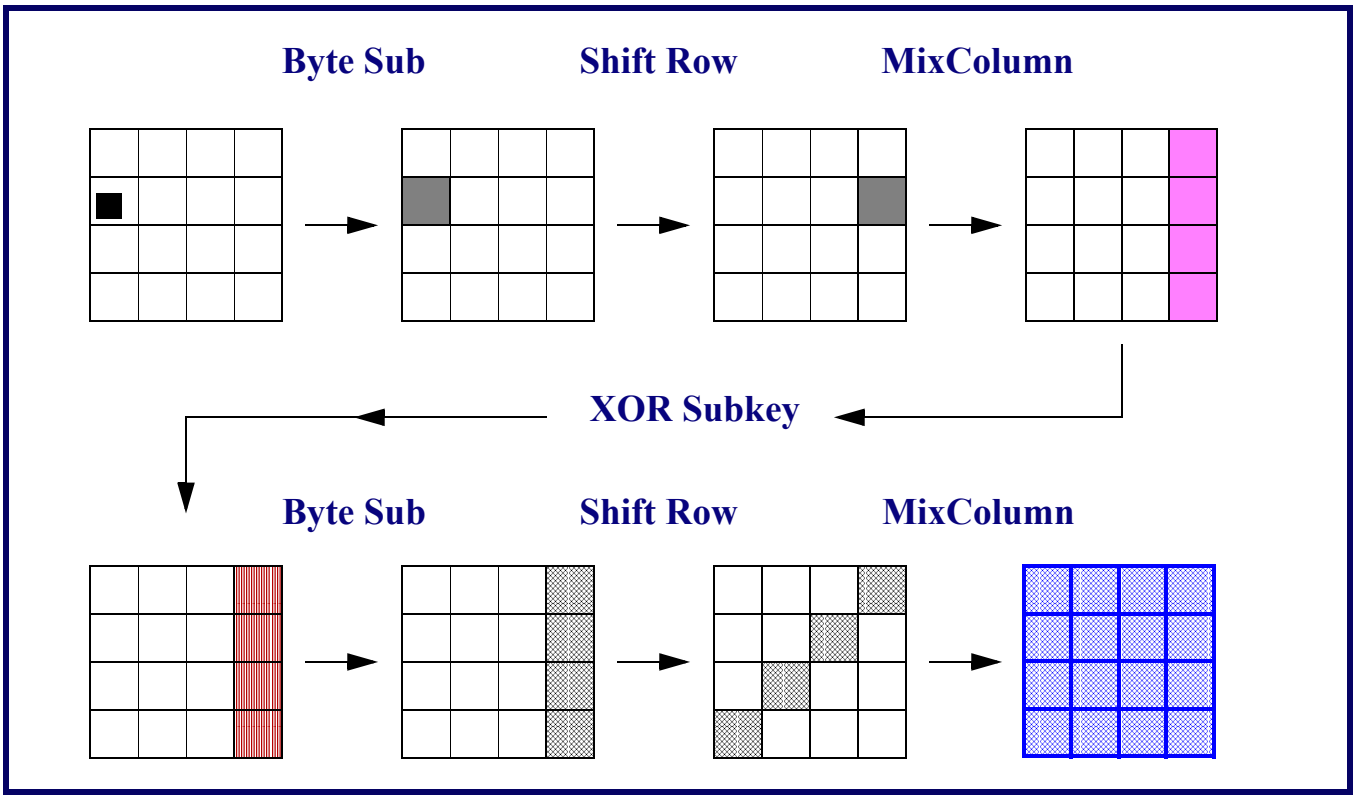
After all that, each word (column) is XORed with a word of the subkey for that round.

So, tell me again what that all meant?

The purpose of the cipher is to change, mix, change again, mix some more . . . until it is impossible to figure out the original input block. Consider two data blocks that start off identically (this is the essence of differential cryptanalysis). Now, suppose that a single bit of one block was changed. Let's look at what happens to the difference in the rest of the data block as the various round operations make modifications based on it.

First, the single bit change means that a different entry in the S-box is selected by ByteSub for that byte, and so there will be very little relationship between the original value and the new one. Effectively, the whole byte has changed significantly, as illustrated in Figure 2.

Figure 2: XOR Subkey Diagram



The first ShiftRow doesn't do much at all, but that's OK. It doesn't matter in which column the altered byte appears. The MixColumn operation will spread out the difference vertically, affecting all the bytes in that column. The shading in the diagram isn't meant to imply that the same change appears in all bytes – it doesn't – it's just meant to imply that the same thing causes the changes.

Up to this point, someone who doesn't know the key can track everything that's happened. But now, some of the subkey material is XORed into the column. The next ByteSub operation will change these values wildly, with a different result for each possible value of the key bytes, and the hypothetical attacker's troubles begin. The next ShiftRow ensures that these changes appear in each column, and the MixColumn then spreads out the effect of the change through the entire block. This behavior is called avalanche, and it's very desirable in an encryption algorithm.

That's only the effect of two partial rounds. By the time all 10 are taken into account, and bearing in mind that the initial whitening means that the attacker can't even track the effect of the first ByteSub, it's obvious that the data block is pretty thoroughly obscured.

Summary

Rijndael is expected to be the encryption standard for at least 20 years. It has been studied more extensively than any other cipher, except DES. In the wireless world, it will be used for privacy in cdma2000 systems, and it is the basis of the recommended Authenticated Key Agreement (AKA) algorithm MILENAGE for W-CDMA (UMTS) systems. As more Internet Protocol functionality appears in mobile phones, its use as the basis of IPSec will also be extensive. Most importantly, Rijndael is an elegant and understandable cipher.

About the Author

Greg Rose is a Principal Engineer for QUALCOMM International, based in Australia, where he works on cryptographic security and authentication for third-generation mobile phones and other technologies. He holds a number of patents on cryptographic methods, and he has successfully cryptanalyzed widely deployed ciphers.

Fraud And Security Patent News

The US Patent and Trademark Office (USPTO) recently granted the following 12 fraud and security patents. The patent number, invention title, inventor, and assignee (owner) are provided. All of these patents were granted in either August or September 2001.

These may be of interest to some of our wireless security practitioners. With the listing below, one can see who is doing what in the world of inventions. Moreover, it is often instructive to read issued patents, the references cited or other references included in the patent. For select patents provided below, we provide the URL and contact information for the assignee.

US Patent: 6,286,103

(Issued: September 4)

Method and apparatus for encrypted data stream transmission

Inventor: Michel Maillard et. al.

Assignee: Canal+Societe Anonyme (Paris, France)

US Patent: 6,286,099

(Issued: September 4)

Determining point of interaction device security properties and ensuring secure transactions in an open networking environment

Inventor: Glenn Kramer

Assignee: Hewlett-Packard Company

US Patent: 6,285,873

(Issued: September 4)

Method for generating a broadcast challenge value [for cellular authentication]

Inventor: Roy (Frank) Quick, Jr.

Assignee: Qualcomm Incorporated

www.qualcomm.com

Contact:

Qualcomm Incorporated
5775 Morehouse Drive
San Diego, CA 92121

Telephone: (858) 587-1121

About:

QUALCOMM, Inc. is engaged in developing and delivering digital wireless communications products and services based on the Company's CDMA digital technology. The Company's business areas include integrated CDMA chipsets and system software; technology licensing; Eudora email software for Windows and Macintosh computing platforms; satellite-based systems including portions of the Globalstar system and wireless fleet management systems, OmniTRACS and OmniExpress.

US Patent: 6,285.871

(Issued: September 4)

Cellular Fraud Prevention using Selective Roaming

Inventor: David Daniels

Assignee: Cellco Partnership (Bedminster, NJ)

US Patent: 6,285,869

(Issued: September 4)

Method for performing replacement of a subscriber identity module (SIM) in a mobile communications network

Inventors: John Shannon and Andrew Morgan.

Assignee: Nortel Networks

US Patent: 6,285,776

(Issued: September 4)

Methods for identifying equipment used in counterfeiting

Inventor: Geoffrey Rhoads

Assignee: Digimarc Corporation

www.digimarc.com

Contact:

Digimarc Corporation
19801 SW 72nd Ave. Suite 100
Tualatin, OR 97062

Telephone: (503) 885-9699
(or toll-free at 800-DIGIMARC)

About:

Digimarc Corporation is a provider of digital watermarking technologies that allow an imperceptible digital code to be embedded in the printed or digital versions of media content, such as commercial and consumer photographs, movies, music, magazine advertisements, catalogs, product packages, and valuable documents, including financial instruments, passports and event tickets.

US Patent: 6,282,658

(Issued: August 28)

System and method for authentication of network users

Inventors: Jennifer French and Jone Wilder

Assignee: Equifax, Inc.

US Patent: 6,282,648

(Issued: August 28)

Method and apparatus for secure measurement certification

Inventor: Jay Walker et. al.

Assignee: Walker Digital, LLC.

www.walkerdigital.com

Contact:

Walker Digital
5 High Ridge Park
Stamford, CT 06905

Telephone: (203) 461-7000

About:

Walker Digital is an integrated business solution invention and development company. Walker Digital's mission is to reinvent and improve businesses through the creative application of new

digital technologies, especially the Internet. Walker Digital has received over 70 U.S. patents and has a portfolio of over 400 patents pending.

US Patent: 6,282,522

(Issued: August 28)

Internet payment system using smart card

Inventor: Virgil Davis et. al.

Assignee: Visa International Service Association

US Patent: 6,282,295

(Issued: August 28)

Auto-recoverable and auto-certifiable cryptosystem using zero-knowledge proofs for key escrow in general exponential ciphers

Inventors: Adam Young and Marcel Yung.

Assignee: same

US Patent: 6,278,781

(Issued: August 21)

Wireless telephony with steganography

Inventor: Geoffrey Rhoads

Assignee: Digimarc Corporation

US Patent: 6,275,806

(Issued: August 14)

System method and article of manufacture for detecting emotion in voice signals by utilizing statistics for voice signal parameters

Inventor: Valery Pertrushin

Assignee: Andersen Consulting, LLP.

US Patent: 6,273,339

(Issued: August 14)

Tamper resistant smart card and method of protecting data in a smart card

Inventor: John Tuttle et. al.

Assignee: Micron Technology, Inc.

www.micro.com

Contact:

Micron Technology, Inc.
8000 South Federal Way
Post Office Box 6
Boise, Idaho 83707-0006

Telephone: (208) 368-4000

About:

Micron Technology, Inc. and its subsidiaries manufacture and market DRAMs, very fast SRAMs, Flash Memory, other semiconductor components and memory modules.

To review the specification and claims of these patents visit the US Patent and Trademark Office web-site at www.uspto.gov. To obtain a complete copy of these patents, contact the US Patent and Trademark Office, at the address or telephone numbers below:

General Information Services Division
U.S. Patent and Trademark Office
Crystal Plaza 3, Room 2C02
Washington, DC 20231

800-786-9199 or 703-308-4357