The Mathematics of Internet Security: Keeping Eve The Eavesdropper Away From Your Credit Card Information

Sean Sather-Wagstaff

Department of Mathematics
North Dakota State University

16 September 2010
Science Cafe

Introduction

Disclaimer:

Sean Sather-Wagstaff is not an internet security expert.

Sean Sather-Wagstaff is an algebra expert.

Ideas:

1. Some aspects of internet security are based on algebra:
prime numbers, factorization, modular arithmetic

2. Security depends on the following fact:
some mathematical operations are easy to do and hard to undo.

Security?

The Internet:

Transmit a message m from computer A to computer B.

A: Alice

B: Bob

m: message
represented as an integer (whole number) $m \geq 0$

The Problem:

How to keep Eve the eavesdropper from knowing m?

What is it?

An algorithm for “public-key cryptography”

Ron Rivest, Adi Shamir, and Leonard Adleman (1978)

Principle of RSA:

Certain mathematical operations are computationally easy to do and computationally difficult to undo.

Example:

Multiplication is computationally easy.

Factorization is computationally difficult.

This is the first essential fact that makes RSA secure.

Modular Arithmetic

Clock arithmetic

Question: If it is 7:00 now, what time will it be in 9 hours?

Answer: 4:00

Solution: $7 + 9 = 16$

Now subtract multiples of 12 to get back to "clock numbers".

$16 = 16 - 12 = 4$

Modular arithmetic:

Let n be an integer (whole number) $n \geq 2$

$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

Addition and multiplication are defined "modulo n":

Add and multiply as usual, then subtract multiples of n to find an answer between 0 and $n - 1$.

Modular Arithmetic (cont.)

Example:

Compute the powers of 4 in $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$:

$$4^1 = 4 \qquad 4^3 = 4 \cdot 4^2 = 4 \cdot 6 = 24 = 4$$

$$4^2 = 16 = 6 \qquad 4^4 = 4 \cdot 4 = 16 = 6$$

etc.

The point:

Computing powers in $\mathbb{Z}_n$ is computationally easy.

Computing "roots" is computationally difficult:
Given m^e in $\mathbb{Z}_n$, it is difficult to figure out what m is.

This is the second essential fact that makes RSA secure.

RSA: The Algebra

Theorem: Choose two distinct prime numbers p and q.

Set $n = pq$ and $\phi = (p-1)(q-1)$.

Find a prime number $e < \phi$ that is not a factor of ϕ.

Find an integer $d < \phi$ such that $de = 1$ in $\mathbb{Z}_\phi$.

Then for all m in $\mathbb{Z}_n$, we have $m = m^{ed} = (m^e)^d$ in $\mathbb{Z}_n$.

Example: $p = 5$ and $q = 7$.

Then $n = 5 \cdot 7 = 35$ and $\phi = 4 \cdot 6 = 24$.

$e = 5$ is a prime number less than 24 that is not a factor of 24.

$d = 5$ is a positive integer such that $ed = 1$ in $\mathbb{Z}_{24}$.

With $m = 2$ we have $m^e = 2^5 = 32$ and (computing in $\mathbb{Z}_{35}$):

$$(m^e)^d = 32^5 = 33,554,432 = 958,698 \cdot 35 + 2 = 2 = m.$$

RSA: Using The Theorem To Encrypt And Decrypt

Alice wishes to transmit a message m securely to Bob.

Bob chooses n, e, and d as in the theorem.

e: the encrypting key

d: the decrypting key

Bob makes the numbers n and e public. Hence, "public key".

Bob keeps d secret.

Encryption: Alice computes $c = m^e$ in $\mathbb{Z}_n$ and sends c to Bob.

c: the coded message

Decryption: Bob recovers m from c by computing in $\mathbb{Z}_n$:
$c^d = (m^e)^d = m$

These steps are computationally easy

RSA: What Makes It Secure?

Eve has the codeword $c = m^e$; she wants m.

Without knowing d, it is computationally difficult to find m.

To find d, Eve needs to know ϕ, so she needs to factor n.

The factorization problem is computationally difficult.

In practice, p and q are 1024-bit or 2048-bit.

1024-bit: $p, q \approx 2^{1024} \approx 10^{308}$ and $n \approx 10^{616}$.

2048-bit: $p, q \approx 2^{2048} \approx 10^{616}$ and $n \approx 10^{1232}$.

There are about 10^{80} atoms in the known universe.

Est. time to factor 1024-bit integer using 8.4 million PC's: 2 yrs.

Record: 768-bit integer factored summer 2005 to Jan. 2010.
1,675 years of operation on a 2.2 GHz Opteron processor

Conclusion

1. Some aspects of internet security are based on algebra: prime numbers, factorization, modular arithmetic

2. The security of RSA depends on the fact that certain mathematical operations are computationally easy to do and computationally difficult to undo.

multiplication is easy, factorization is hard

exponentiation is easy, taking roots in $\mathbb{Z}_n$ is hard