MATH 253: IN-CLASS RSA EXERCISE

DAN YASAKI

1. Some history

Rivest, Shamir, and Adleman first publicly described this algorithm for public key encryption in 1978[1]. They posted one of the first public-key encryption messages using a 129 digit number which later became known as RSA-129.

They offered a $100 prize and remarked that using technology and factoring techniques available at that time, it would take 40 quadrillion years to crack. Advances in factoring techniques and computers cracked the code to find that the secret message was:

The Magic Words are Squeamish Ossifrage

According to Wiki,

> Ossifrage is an older name for the lammergeier, a scavenging vulture that is famous for dropping animal bones and live tortoises onto rocks to crack them open. It might perhaps be considered among the least squeamish of creatures.

2. The set-up

The *RSA public encryption key* consists of a pair of integers (N, e). The set of integers $\{1, \cdots, N\}$ is the set of possible messages. To encrypt a message M, you compute

$$C \equiv M^e \pmod{N}.$$

If a Eve captures C while it is being transmitted, she will have a hard time computing the original message M. See Section 2 for more information. How is it any easier for me, if I am the one that constructed the key? The trick is that I have a bit of extra information. When constructing the key, I choose N to be a product of two distinct primes p and q. The exponent e is chosen so that $\gcd(e, \phi(N)) = 1$. Then using the Euclidean algorithm, I can compute d such that $ed \equiv 1 \pmod{\phi(n)}$. Then there is an integer k so that $ed = 1 + k\phi(N)$. Now Euler says that if $(C, N) = 1$,

$$\begin{aligned} C^d &\equiv (M^e)^d \pmod{N} \\ &\equiv M^{1+k\phi(N)} \pmod{N} \\ &\equiv M \cdot (M^{\phi(N)})^k \pmod{N} \\ &\equiv M \pmod{N}. \end{aligned}$$

In other words, to decrypt the message, I do not need to take an e^{th} root of C modulo N. I can raise C to the d power and achieve the same result. Thanks Euler.

[1]Clifford Cocks described an equivalent system in 1973, but it was classified by the UK intelligence agency GCHQ until 1997

3. Example

Suppose I have public key $(N, e) = (55, 3)$. Then you can encrypt any number from 1 to 55. Suppose you wish to encrypt your guess for my age. (I am clearly younger than 55, so this message space is large enough.) For the purposes of this exercise, suppose you think I am 18 :)

You set $M = 18$. You need to compute $C \equiv M^e \equiv 18^3 \pmod{55}$. A quick computation gives $C = 2$.

How do I decrypt? I know that $\phi(55) = 40$, since I chose a value for N that I could factor. The decryption exponent d satisfies $ed \equiv 1 \pmod{\phi(N)}$. I compute

$$\begin{aligned} 3d &\equiv 1 \pmod{40} \\ d &\equiv -13 \pmod{40} \end{aligned}$$

by extended Euclidean Algorithm

q	r	s	t
	40	1	0
13	3	0	1
3	1	1	−13
	0	−3	40

or by observing that $3 \cdot 13 = 39 \equiv -1 \pmod{40}$.

I can take $d = 27$ since $27 \equiv -13 \pmod{40}$. To decrypt $C = 2$, I must compute

$$\begin{aligned} M &\equiv C^d \pmod{N} \\ &\equiv 2^{27} \pmod{55} \\ &\equiv 18 \pmod{55} \end{aligned}$$

What are some of the problems with this example? i.e. What kind of attacks should Eve try?

(1) If Eve could solve $x^3 \equiv 2 \pmod{55}$, she can find your guess. The message space 55 is small enough that she could just compute $x^3 \pmod{55}$ for several values of x and quickly find an answer.

(2) The value $N = 55$ is too easy to factor. Once she knows $55 = 5 \cdot 11$, CRT tells her that

$$\phi(55) = \phi(5)\phi(11) = (5-1)(11-1) = 40.$$

Then she can compute d using Euclidean algorithm just as we did to decrypt any intercepted message.

4. Why is RSA secure?/What numbers should I pick?

The encryption key e is typically chosen to be $e = 2^{16}+1 = 65537$. This is not for security, but for speed. Because of our fast powering algorithm, this choice of e allows encryption to be done quickly.

If p and q are chosen to be *large* primes (for today's technology 100-200 digit primes are large enough), then the claim is that this encryption is secure. To decrypt a message, you either have to be able to take e^{th} roots (i.e. solve $x^e \equiv C \pmod{N}$), or compute d. The first

problem is HARD, and one of the main ways to try to solve it is via finding d. In order to find d, you must know $\phi(N)$. As long as I keep the factors p and q secret then computing $\phi(N)$ is HARD.

5. ASCII

ASCII is a standard way to represent characters as numbers. For example, a space is represented by 32, a comma is 44, and a period is 46. The capital letters are also 2 digit integers, and are given below.

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

6. Practice

For this class exercise, my RSA public encryption key is

$$(N, e) = (629, 17).$$

(Note that $17 = 2^4 + 1$.)

(1) Encrypt the letter A by converting to ASCII, then encrypting using my public key. (You should get 337.)

(2) I have encrypted a short message. Can you break RSA to read the message? Each cipher-text represents 1 letter. (Note: You can try to break RSA by factoring my public key N. That is the way I would like you to approach this. Do you see a way to crack this one without factoring? It is vulnerable since the message space is so small.)

My secret message is

$$247, 337, 322, 463, 15, 73, 440, 15, 342, 323, 435$$

Department of Mathematics and Statistics, The University of North Carolina at Greensboro, Greensboro, NC 27402-6170, USA

E-mail address: d_yasaki@uncg.edu