Chapter 3

The RSA

R S A

It seems like a small step from the previous cipher to this one, but the improvement is gigantic. Notice how this is like and differs from the previous one

Number theory result. Let p and q be distinct primes and $n = pq$
The multiples of p up to $n = pq$ are
$p \quad 2p \quad 3p \qquad qp = n$
The multiples of q up to $n = pq$ are
$q \quad 2q \quad 3q \qquad pq = n$
These numbers are not relatively prime to n. There ar $p+q-1$ of them.
The numbers relatively prime to n are $n-(p+q-1) = pq-(p+q-1) = (p-1)(q-1)$

Let $m = (p-1)(q-1)$ and e be relatively prime to m. Hence there exists d such that $ed \equiv 1 \bmod m \rightarrow$
$ed = 1 + km$ for some k
If $\gcd(x, p) = 1 \rightarrow$
$x^{ed} = x^{1+(p-1)(q-1)k} = x(x^{p-1})^{k(q-1)} \bmod p = x \bmod p$
If $\gcd(x, q) = 1$, we get $x^{ed} = x \bmod q$ in the same way.
If $\gcd(x, p) \neq 1 \rightarrow p \mid x$ as $x \equiv 0 \bmod p \rightarrow$
$x^{ed} \equiv x \bmod p$. Same for q
So $x^{ed} \equiv x \bmod p \quad x^{ed} \equiv x \bmod q$

Hence p and q divide $x^{ed}-x$

Since p and q are distinct primes, pq divides $x^{ed}-x \Rightarrow$

$$x^{ed} \equiv x \bmod n$$

This idea is the basis for the RSA

The RSA

Alice picks primes p and q $(p \neq q)$

Let $n = pq$ $\quad m = (p-1)(q-1)$

She finds e with $\gcd(m, e) = 1$

So she finds d with $ed \equiv 1 \bmod m$

Alice makes public (n, e)

That is her public key

m and d are her private key

She must keep secret p, q, m and d for if ~~she~~ Eve knows any of them, she knows d.

Bob wants to send message x to Alice. He compute $x^e \bmod n = y$ and sends y, the ciphertext, to Alice. She computes $y^d = x^{ed} = x \bmod n$ to get Bob's message.

Eve knows n, e and y. To get x, she needs d. The point is that knowing n, e and it is very hard to find d and so x.

3

Eve also knows n. If she can find p or q, she can compute $m=(p-1)(q-1)$ and use m and e in the Euclidean algorithm to find d and break the system. It is a factoring problem of a big integer which makes the RSA very secure, at least in this day and age. There is a lot of work done on factoring a big n. We will look at some

Ex ~~Bo~~ Alice picks $p=3$, $q=11$, $e=7$
Find d. She makes $(n, e)=(33, 7)$ public. Bob wants to send her the name of his favorite Blues artist

B B K I N G

$x=$ 1 1 10 8 13 6

He computes $x^e \bmod n = y$ getting

$y=$ 1, 1, 10, 2, 7, 30

He send this to Alice
Alice computes $y^d \bmod n$ for each y to learn of his favorite

Problems

(1) Find the inverse of 34 mod 55 using the Euclidean algorithm

(2) Find: a 3^{25} mod 50

b 13^{30} mod 31

c 13^{31} mod 31

(3) Alice and Bob use the exponential cipher with $p = 29$ and $e = 5$
Find d. Alice sends Bob

15 0 15 16 0 14 17

what is her message?

(4) Alice sets up the RSA with $p = 3$ $q = 11$ $e = 3$. what is d?
She puts $(e, n) = (3, 33)$ for anyone to use
Bob uses it and sends
27 29 12 0 19 27 30 8 11 13 31 19
as his ciphertext. what is his message?

(5) Alice picks $p = 5$, $q = 7$ $e = 5$
and makes $(35, 5) = (n, e)$ public
Bob sends 12, 9, 0, 6, 0, 13 Find the message

(6) Find d if $p = 11$, $q = 17$, $e = 27$

RSA RELATED RESULTS

SIGNATURES

A process considered as important as sending messages is the concept of signatures. Most cryptosystems also have signature schemes. The idea is if Alice sends Bob a message Bob wants to be certain that it came from Alice.

Here we use RSA ideas to look at the signature problem.

Suppose that the message itself does not need to be secret but it is important to know who sent it

Suppose x is the message that Alice is sending. She used her RSA setup: p q m n e d where n and e are public. She computes $x^d \bmod n = y$ and sends x and y to Bob. Bob computes $y^e \bmod n = x$ and verifies that Alice sent the message (only Alice knows d to get the y that $y^e \bmod n = x$.

Or perhaps the message x needs to be kept secret. Then Alice and Bob use both of their RSA setups. To distinguish them, we will use subscripts

Alice: p_A q_A n_A m_A e_A d_A

Bob: p_B q_B n_B m_B e_B d_B

What is public is (n_A, e_A) (n_B, e_B)

Alice computes

$$x^{d_A} \bmod n_A = y$$

and

$$y^{e_B} \bmod n_B = z$$

and sends z to Bob

Bob computes $z^{d_B} \bmod n_B = y$

and $y^{e_A} \bmod n_A = x$

to get both the message and the assurance that Alice sent it

Computation note: Bob needs to take care in the order that he does the computation. He knows both n_A and n_B. He should use the smaller of the two last.

Ex Alice picks

$p_A = 5 \quad q_A = 3 \quad n_A = 15 \quad m_A = 8 \quad e_A = 3 \quad d_A = 3$

Bob picks

$p_B = 7 \quad q_B = 2 \quad n_B = 14 \quad m_B = 6 \quad e_B = 5 \quad d_B = 5$

Alice is going to send 2 to Bob

She compute $2^5 \bmod 14 = 4 = y$

$4^3 \bmod 15 = 4 = z$

and sends $z = 4$

Bob computes $4^3 \bmod 15 = 4 = y$

$4^5 \bmod 14 = 2$

FACTORING

If $n = pq$ and n is known, can p and q be found. If so, this would break an RSA problem using those numbers. There are many methods, some very old we look at several of them

FERMAT FACTORING

Suppose $n = pq$

Let $x = \frac{p+q}{2}$ $\quad y = \frac{p-q}{2}$

Then $pq = (x+y)(x-y) = x^2 - y^2 \quad (x > y)$

Let x be the smallest integer greater than $\sqrt{n}$. Compute $y^2 = x^2 - n = x^2 - pq$

If y is an integer, then $p = x+y$ and $q = x-y$ solve the problem

If not, replace x by $x+1$ and try again. Keep this up as long as you want. If x and y are close to each other, the

method will work. This is to say if p and q are close together this method will work.

Ex $n = 64349$

$253 < \sqrt{n} < 254$

Let $x = 254$

$x^2 - n = 167$ is not a square

$x = 255$

$x^2 - n = 676 = 26^2 = y^2 \rightarrow$

$y = 26$ Then

$p = x + y = 255 + 26 = 281$

$q = x - y = 255 - 26 = 229$

The Pollard ρ

This method is due to J.M. Pollard who has several clever algorithms for this material

Problem: Factor n

Let $f(x)$ be an irreducible polynomial in the rationals. Say $f(x) = x^2+1$

Pick $x_0 =$ integer

Compute $x_1 = f(x_0) \bmod n$

$x_2 = f(x_1) \bmod n$

$\vdots$

$x_{t+1} = f(x_t) \bmod n$

There must be a repition after $n+1$ steps. If p divides n then the $x_i \bmod p$ must repeat after $p+1$ steps. Of course we can't see it since we do not know p. Let

$\bar{x}_j = x_j \bmod p$

Suppose $\bar{x}_j = \bar{x}_i$ for some $i, j, i \neq j$

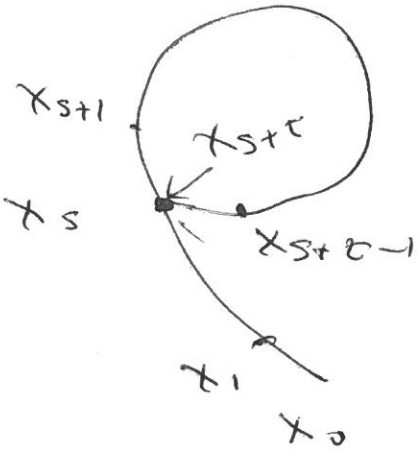
Then $p \mid x_j - x_i \rightarrow$

$$p \mid \gcd(n, x_j - x_i) = d$$

If $d < n$, then d is a factor of n

If $d = n$, start again with another x_0 (or $f(x)$)

Geometrically, it looks like



So $x_{s+t} \equiv x_s \mod p$

At this point, we need to check the gcd's of n and every $x_j - x_i$, a lot of steps

Instead we could compute $\gcd(n, x_2 - x_1)$, $\gcd(n, x_4 - x_2)$, $\gcd(n, x_6 - x_3)$ ... $\gcd(n, x_{2j} - x_j)$

In doing this 2 things happen

We move along the ρ, one step at a time and we increase the distance between x's one step at a time. Eventually we will be one the circle part of the ρ and we will be at the place where the x_i and x_j land on each other, like at x_s and $x_{s+\tau}$.

Ex $n = 1133$ Let $x_0 = 2$ $f(x) = x^2+1$

Compute $x_i = f(x_{i-1}) \bmod n$.

We get

2, 5, 26, 677, 598, 710, 1049, ...

Do the gcd's

$\gcd(x_2 - x_1, n) = \gcd(26-5, n) = 1$

$\gcd(x_4 - x_2, n) = \gcd(598-26, n) = 11$

So 11 is a factor.

Ex. $n = 82123$ $f(x) = x^2+1$ $x_0 = 630$

41 is a factor. We make a table listing $x_i \bmod n$ and $x_i \bmod 41$

i	$x_i \bmod n$	$x_i \bmod 41$
0	631	16
1	69670	11
2	28926	40
3	69907	2
4	13164	5
5	64027	26
6	40816	21
7	80802	32
8	20459	0
9	71874	1
10	6688	2
11	14314	5
12	75835	26
13	37282	21
14	17531	32

Note the $p=41$ column repeats at $i=3$ and $i=10$ and theafter

We would find a match when $i=14$ and $i=7$

$\gcd(x_{14}-x_7, n) = 41$

Note we never see the last column

PRIMALITY TESTS

Another problem associated with the R.S.A is whether an integer is prime. A fundamental property is shown in FERMAT'S THEOREM that was discussed before. Notably

FERMAT: If p is a prime and a is an integer with $\gcd(a,p)=1$, then $a^{p-1} \equiv 1 \bmod p$

Ex. Let $p=6$ Then $2^5 = 32 \equiv 2 \bmod 6$ so p is not prime.

However, there are integers p such that $a^{p-1} \equiv 1 \bmod p$ but p is not a prime. The smallest such number is $p = 341$. Then it can be computed that $2^{340} \equiv 1 \bmod 341$

Note that $341 = (31)(11)$

Definition: If n is a composite number and a is an integer with $\gcd(a,n)=1$ and $a^{n-1} \equiv 1 \bmod n$, then n is called a pseudoprime base a

341 is a pseudoprime base 2 But not base 3 as $3^{340} \not\equiv 1 \bmod 341$.

So one would hope that if n is not a prime, trying a number of a's will show it. But this is not the case

Ex $n = 561 = 3 \cdot 11 \cdot 17$, has $a^{n-1} \equiv 1 \bmod n$ for all a with $\gcd(a,n)=1$. Such a number is called a Carmichael number

Some properties of Carmichael numbers

1. If n is divisible by a square then it is not a Carmichael number
2. If n is square free, then n is a Carmichael number if and only if $p-1 \mid n-1$ for every prime p that divides n

3. A Carmichael number must be the product of at least 3 primes

Note that $561 = 3 \cdot 11 \cdot 17$ and

$3-1 \mid 561-1$

$11-1 \mid 561-1$

$17-1 \mid 561-1$

Remarks

Pseudoprimes base 2 less than 1000 are 341, 561, 645

Pseudoprimes base 2 less than 1,000,000 are in number 245 versus 78498 primes. So they are rare.