

L E S S O N 12

THE RSA

# R S A

I A result of Fermat

Thm. If  $p$  is a prime and  $p$  does not divide  $e$ , then  $e^{p-1} \equiv 1 \pmod{p}$

Proof, let  $S = \{1, 2, \dots, p-1\}$   
Then  $eS = \{e, 2e, \dots, (p-1)e\} \pmod{p}$

If  $e_i \equiv e_j \pmod{p}$ , then

$e_i(e_i - j) \equiv 0 \pmod{p}$  and

$p$  divides  $e_i(e_i - j)$

$p$  does not divide  $e$ ,

hence  $p$  divides  $e_i - j$

$\rightarrow i \equiv j \pmod{p}$

So the mapping

$S \rightarrow eS, i \rightarrow ei \pmod{p}$

is  $1-1$ , hence it is onto

since  $S$  is a finite set,

so  $eS \pmod{p}$  has the same

elements as  $S$ , just arranged  
differently, so the product

of all elements in  $S$  = the

product of all elements in

$eS \pmod{p} \rightarrow (p-1)! = e^{p-1}(p-1)! \pmod{p}$

$\rightarrow (e^{p-1}-1)(p-1)! \equiv 0 \pmod{p} \rightarrow$

$p$  divides  $e^{p-1}-1 \rightarrow e^{p-1} \equiv 1 \pmod{p}$

2

Thm. Suppose  $\gcd(e, p-1) = 1$   
 Then there exists  $d$  such that  
 $ed \equiv 1 \pmod{p-1}$  ⑥  
 Then  $a^{ed} \equiv a^{1+k(p-1)} \equiv a \pmod{p}$   
 Proof The first result holds  
 because  $e$  and  $p-1$  are  
 relatively prime and  $d$   
 can be found using the  
 Euclidean algorithm Table.

Suppose  $\gcd(a, p) = 1$ .  
 Then  $a^{ed} \equiv a^{1+k(p-1)} \pmod{p}$   
 $= a(a^{p-1})^k \pmod{p} = a$  (using the  
 last Thm)  $\equiv a \pmod{p}$   
 Suppose  $\gcd(a, p) \neq 1$ . Since  
 $p$  is prime,  $\gcd(a, p) = p$   
 and  $p$  divides  $a$   
 so  $a^{ed} \pmod{p} = 0 \pmod{p} = a \pmod{p}$

These facts allow us to  
 construct a cipher, the  
 exponential cipher. It is  
 a predecessor of the RSA  
 but is only a private key  
 system.

Exponential Ciphers  
 Alice and Bob pick a prime  
 $p$  and  $e$  with  $\gcd(e, p-1) = 1$

3

They find  $d$  such that  
 $e d \equiv 1 \pmod{p-1}$  (Euclidean algorithm)  
Bob wants to send  
message  $a$  to Alice  
He computes  $b = a^e \pmod p$   
and sends  $b$  to Alice  
Alice computes  
 $b^d = a^{ed} \pmod p = a \pmod p$  to  
get the message  
If Eve knew  $e$ , she  
could find  $d$ . Since  
she does know  $b$  (it was  
sent), she computes  $b^d$  to  
get  $a$  just like Alice did.  
So  $e$  can not be made public.  
This problem will be  
erased in the RSA

4

Ex

Bob and Alice pick  $p=181$  and  $e=97$ . Note that  $\gcd(e, p-1)=1$ . They compute  $d=28$ , so  $ed \equiv 1 \pmod{p-1}$

Bob wants to send

B E T R A Y A L  
1 4 19 17 0 24 0 11

to Alice. Each of these numbers will be a in  $b \equiv a^e \pmod{p}$

By repeated squaring (or a calculator), the b's are

1 94 19 92 0 158 0 168

This is the ciphertext that is sent to Alice. She computes  $b^d \pmod{p}$  ( $d=28$ ) to get the original numbers (the plaintext) and converts them to numbers to get the message.

## RSA

It will seem like a small step from the previous cipher to the RSA, but the ramifications are enormous. The RSA is a famous public key system. The initials are for its developers

RIVEST SHAMIR ADELMAN who developed it at M.I.T.

## Number Theory Result

This result takes the place of the Theorems in the last section.

Let  $p$  and  $q$  be distinct primes and  $n = pq$ . The multiples of  $p$  up to  $n$  are

$$p, 2p, 3p, \dots, qp = n$$

Likewise, the multiples of  $q$  are

$$q, 2q, 3q, \dots, pq = n$$

These are the numbers less than or equal to  $n$  that are not relatively prime to  $n$ . There are

$$p + q - 1$$

of them by checking the lists

6

So the remaining numbers less than  $n$  are relatively prime to  $n$  and there are

$$n - (p+q-1) = pq - (p+q-1) = (p-1)(q-1)$$

of them. Let

$m = (p-1)(q-1)$  and  $e$  be relatively prime to  $m$ .

Hence there exists  $d$  such that  $ed \equiv 1 \pmod{m}$   $\rightarrow$

$$ed = 1 + km \text{ for some } k$$

$$\begin{aligned} \text{If } \gcd(x, p) = 1 \rightarrow \\ x^{ed} &\equiv x^1 + (p-1)(q-1)k = x(x^{p-1})^{k(q-1)} \pmod{p} \\ &= x \quad (\text{by Fermat}) \end{aligned}$$

In the same way, if  $\gcd(x, q) = 1 \rightarrow$

$$x^{ed} \equiv x \pmod{q}$$

If  $\gcd(x, p) \neq 1$ ,  $p$  divides  $x$  and  $x^{ed} \equiv 0 \pmod{p} = x \pmod{p}$  and the same for  $q$ .

So  $x^{ed} \equiv x \pmod{p}$   $x^{ed} \equiv x \pmod{q}$  for any  $x$ . So  $p$  and  $q$

divide  $x^{ed} - x$ . Since  $p$  and  $q$  are distinct primes,  $pq$  divides  $x^{ed} - x$  and we get the point:

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

We can use  $e$  and  $d$  in this system as we did in the last one.

## The R. S. A.

Alice picks distinct primes  $p$  and  $q$ . Let  $n = pq$ ,  $m = (p-1)(q-1)$ . She picks  $e$ ,  $\gcd(e, m) = 1$ . She finds  $d$ ,  $e^d \equiv 1 \pmod{m}$ .

Alice makes public  $(n, e)$ . That is her public key  $m$  and  $d$  are her private key and they, along with  $p$  and  $q$  are known only to Alice.

The rest is like the exponential cipher. Bob wants to send message  $x$  to Alice. He computes  $y = x^e \pmod{n}$  and sends ciphertext  $y$  to Alice. She computes  $y^d = x^{ed} \pmod{n} = x$  to get his message.

Eve knows  $e$  and  $n$ . If she can factor  $n = pq$  to get  $p$  and  $q$ , she can get  $m = (p-1)(q-1)$  and the  $d$  from

the Euclidean algorithm. So

Given  $n = pq$ , factor  $n$ . This is very hard in general.

The numbers will be very large. Much research has been done searching for good factoring algorithms. We will look at some of them.

Ex

Alice picks  $p = 3$   $q = 11$ . so  $n = 33$ ,  $m = 22$ . She picks  $e = 7$  so  $\gcd(m, e) = 1$ . She finds  $d = -3 = 19 \pmod{22}$ . Alice make public  $(n, e) = (33, 7)$

Bob wants to send her the name of Blues legend

B B K I N G  
 $x = 1 \ 1 \ 10 \ 8 \ 13 \ 6$

Bob computes  $y = x^e \pmod{33}$ , getting  
 $1 \ 1 \ 10 \ 2 \ 7 \ 30$

and sends them to Alice who computes  
 $y^d \pmod{n}$  getting the message

## PROBLEMS

1. Find the inverse of 34  
 $\text{mod } 55$

2. Find  $3^{25} \text{ mod } 50$   
 $13^{30} \text{ mod } 31$   
 $13^{31} \text{ mod } 31$

3. Alice sets up the RSA  
 with  $p=3, q=11$ . She picks  $e=3$   
 What is  $d$ ?

She sets out her public key  
 $(n, e) = (33, 3)$

Bob uses it to encipher his  
 message, setting

27, 29, 12, 0, 19, 27, 30, 8, 11, 13, 32, 19  
 as his cipher text.

What is his message?

## HOMEWORK 4

For the RSA, Alice picks primes  
 $p=5, q=7$  and public key  $e=5$ .  
 What is  $d$ ? She makes public  
 $(n, e)=(35, 5)$ . Bob uses it to send  
 $18, 14, 32, 8, 0, 16, 33, 8, 18, 6, 0, 32, 8, 13, 6$   
 What is the message?