

MA 437 LESSON 13

RSA SIGNATURE SCHEMES

and

FACTORING

## RSA RELATED RESULTS

### SIGNATURE SCHEMES

A process considered as important as sending secret messages is the concept of SIGNATURES. Most CRYPTOSYSTEMS also have signature schemes. The idea is that if Alice sends Bob a message, they both want to be sure that Alice sent it.

Here we look at RSA signature schemes.

In the first case, suppose that the message does not need to be secret, but it is important to know who sent it.

2

Suppose that  $x$  is the message that Alice is sending. She uses her R.S.A setup:  $p, q, m = (p-1)(q-1)$ ,  $n = pq$ ,  $e$  with  $\gcd(e, m) = 1$  and  $d$  with  $ed \equiv 1 \pmod{m}$ .

Alice computes  $x^d \pmod{n} = y$  and sends both  $x$  and  $y$  to Bob.

Bob uses Alice's public key  $(n, e)$  and finds  $y^e \pmod{n} = x^{de} \pmod{n} = x$  and verifies that Alice sent the message because only Alice knows  $d$  to compute  $y \equiv x^d \pmod{n}$ .

3

Alice picks

$$p_A = 5 \quad q_A = 3 \quad n_A = 15 \quad m_8 = 8 \quad e_A = 3 \quad d_A = 3$$

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 message is  $x = 2$

She computes  $x^{d_A} \bmod n_A = 2^3 \bmod 15 = 8 = y$

She sends  $x = 2$  and  $y = 8$  to Bob

Bob computes  $y^{e_A} \bmod n_A = 8^3 \bmod 15 = 2$

Since this is equal to  $x$ ,  
Alice sent the signature

## FACTORING

## FERMAT

Given  $n = pq$ , find  $p$  and  $q$

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

$$\text{Then } p = x+y, \quad q = x-y$$

$$n = pq = (x+y)(x-y) = x^2 - y^2. \text{ or}$$

$$y^2 = x^2 - n$$

Take  $x$  to be the smallest

integer  $> \sqrt{n}$ . Compute  $y^2 = x^2 - n$

If  $y$  is a perfect square,  
then we have  $x$  and  $y$ , hence  
 $p$  and  $q$ .

If not, step  $x$  by 1 and  
repeat. Repeat this until  $y$   
is a perfect square

6 Ex Let  $n = 64349$

$$253 < \sqrt{n} < 254$$

Let  $x = 254$

$$y^2 = x^2 - n = 167, \text{ not a square}$$

Let  $x = 255$

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

so  $y = 26$

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

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

## FACTORING

## POLLARD

The Pollard  $\rho$ 

Object: Factor  $n$

Say  $p$  is a factor

Let  $f(x)$  be an irreducible polynomial ( $\exists x \ f(x) = x^2 + 1$ )

Let  $x_0 = \text{integer}$

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

$$x_2 = f(x_1) \bmod n$$

$$x_3 = f(x_2) \bmod n$$

:

:

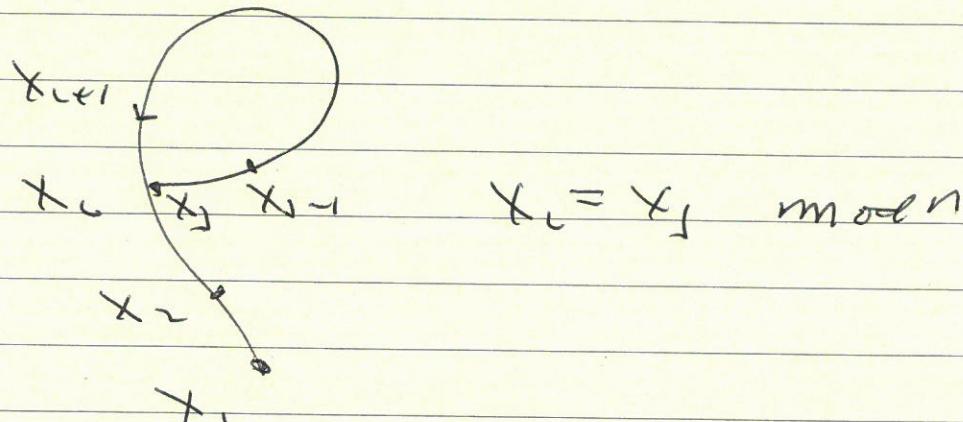
:

In the sequence  $x_1, x_2, \dots, x_n, \dots$   
 we must, all  $\bmod n$ , we  
 must repeat after  $n+1$   
 steps. Although we don't see  
 $x_1 \bmod p, x_2 \bmod p, \dots, x_n \bmod p$   
 we must repeat after  $p+1$   
 steps.

Let  $\bar{x}_j = x_j \bmod p$ ,  $\bar{x}_i = x_i \bmod p$   
 For some  $i, j$ ,  $\bar{x}_j = \bar{x}_i$   
 $\rightarrow x_j \equiv x_i \bmod p$   
 $\rightarrow p \text{ divides } x_j - x_i$

$\rightarrow P$  divides  $\gcd(x_i - x_j, n) = d$   
 So if we can find the  
 correct  $l$  and  $j$  we will  
 get  $\gcd(x_i - x_j, n) \neq 1$ . It  
 could be 1,  $P$ ,  $q$  or  $n$   
 If either  $P$  or  $q$ , we  
 have factored  $n$ . We will  
 get a lot of 1's, so we  
 keep going. If we get  $n$   
 we need to start again.

In computing  $x_1, x_2 \dots$   
 we get the following picture



We get a smaller version of  
 this mod  $p$ .

Remember, we do not know  $p$   
 so we do not see the  
 smaller version, but it  
 exists just the same.

It is important to notice that once  $x_c \equiv x_j \pmod{p}$  then  $x_{c+1} \equiv x_{j+1} \pmod{p}$  and so on. They go around the  $p$  together

To do the computations, up till now, we would need to compute  $\gcd(x_i - x_j, n)$  for all pairs  $(i, j)$ , very time consuming

~~Strategy.~~ We need to get  $x_1, x_2, \dots$  until

1. We get to the circle
2. We get the right cycle

so  $x_c - x_j$  is divisible by  $p$

Instead of  $x_1, x_2, \dots$  we compute  
 $\gcd(x_1 - x_2, n)$   
 $\gcd(x_2 - x_4, n)$   
 $\gcd(x_3 - x_6, n)$

etc

This is moving us up the tail and trying to find the connect cycle length at the same time.

The different  $x_i - x_{i-1}$  keep increasing the different positions by 1 each time.

Ex

$$n = 1133$$

$$\text{Pick } f(x) = x^2 + 1 \quad x_0 = 630 \quad x_0 = 2$$

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

We get

$$2, 5, 26, 677, 598, 710, 1049, \dots$$

The gcds are

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

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

$\rightarrow 11$  divides  $n$  so we have a factor

Ex

$$n = 82123 \quad f(x) = x^2 + 1, \quad x_0 = 630$$

To see what is happening we make a table listing

$x_i \bmod n$  and  $x_i \bmod 41$  since 41 is a factor of  $n$

i	$x_i \bmod n$	$x_i \bmod 41$
0	631	16
1	69670	11
2	28926	40
3	69907	2
4	13166	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

Remember, we do not see the last column.

Note that  $x_3 \bmod 41 = x_{10} \bmod 41$  for the first repetition. This is where the circle in the P starts. Notice that  $x_{3+1} \bmod 41 = x_{10+1} \bmod 41$  from then on. The points are cycling around the P together. The cycle length is  $10 - 3 = 7$ .

12

$\text{gcd}(x_1 - x_3, n)$  would have found the factor 41 but our algorithm did not compute it.

Rather we use

$\text{gcd}(x_4 - x_7, n)$ . This would be 41. So we need to go 4 steps past the first instance but the process saves computing all the intermediate differences. Also note that in practice we do not see the last column.