

# RSA CRYPTOGRAPHY

*John Hutchinson*

## “Simple” Coding Methods.

- Replace Letters by other Letters:  
e.g.  $\{a, b, c, \dots\} \rightarrow \{x, u, b, \dots\}$ .  
Trivial to crack.
- Replace *blocks* of (say) 20 letters by other blocks of 20 letters.  
So many possibilities, hard to crack.  
But if someone steals the “codebook” or machine method (e.g. Enigma) they *can* decode.

## **RSA coding: almost too amazing to be true.**

- Everyone knows how to code; only I know how to decode!!
- This is a *Trapdoor Function*: one direction easy (coding), other essentially impossible (decoding) *without additional information*.

## RSA: Main Features.

- (1) *Messages to Numbers*: Represent secret messages  $M$  as secret numbers, a simple translation,  
 e.g.  $\{a, b, c, \dots\} \rightarrow \{10, 11, 12, \dots\}$  and *back*  $\rightarrow W = 11101220$ .  
 (This is *not* RSA coding).  
 Think of *secret numbers* rather than *secret word messages*
- (2) *Sketch of RSA Method*. I do the following:
- (a) Choose 2 random 150 digit primes (easy)  $p$  and  $q$ .
  - (b) Multiply them, getting  $n = pq$  (easy), which is 299 or 300 digits long
  - (c) Announce  $n$  to the world, but tell nobody what  $p$  and  $q$  are.
  - (d) Tell the world how to code secret numbers  $W$  into coded numbers  $C$ .
  - (e) Use  $p$  and  $q$  to decode  $C$  into  $D$ , which equals  $W$ , and so find  $M$ .
- (3) *So why doesn't someone factor  $n$  to get  $p$  and  $q$ ?*
- (a) Factoring  $n$ : *current* technology – not in lifetime of the universe.
  - (b) *The RSA challenge*:  
<http://www.rsasecurity.com/rsalabs/node.asp?id=2092>  
 Prizes: \$(US)30K for a certain 212 digit number,  
 \$(US)50K for 232 digits, \$(US)75K for 270 digits,  
 \$(US)100K for 309 digits, \$(US)150K for 463 digits,  
 \$(US)200K for 617 digits.

## How Big is Big?

- (1)  $10^{21}$  atoms in a pinhead,  $10^{80}$  atoms in the universe.
- (2)  $10^{22}$  grains of sand on the earth, at least as many stars in the universe.
- (3)  $8.32 \times 10^{81}$  ways of arranging the 60 books on my bookshelf.
- (4) a *googol* is  $10^{100}$ , it is 1 followed by 100 zeros;  
a *googolplex* is  $10^{\text{googol}}$ , it is 1 followed by a googol of 0's.
- (5) Maple will find in a flash the remainder after dividing  $C^d$  by  $n$ ,  
with  $C, d, n$  each bigger than a googol.

## How Does RSA Work?

We temporarily use 50 digit primes for clarity. Not very secure.

*Finding my public and private key.* I do the following:

- (1) Choose two random 50 digit primes  $p$  and  $q$ .  
 (Easy, there are about  $10^{48}$  of them.)  
 $p = 76398256649802838977659276645678008926455022098233$   
 $q = 49290864532859690887375854988876987997867279656387$ .
- (2) Calculate  $n = pq$  and  $m = (p - 1)(q - 1)$   
 $n = 37657361190720787856100500965143810983948577931129$   
 $35004335910637690128606707102326228667007999864171$   
 $m = 37657361190720787856100500965143810983948577931128$   
 $09315214727975160263571575467771231742685698109552$
- (3) Find some  $e$  relatively prime to  $m$ .  $e = 5$  works here.  
 Find the unique  $d$  between 1 and  $m - 1$  for which  $ed = 1 \pmod{m}$ .  
 Here  $d = 1506294447628831514244020038605752439357943117$   
 $245123726085891190064105428630187108492697074279243821$
- (4) Publish my public key  $(n, e)$  in the Canberra Times.  
 Keep my private key  $d$  very secret.

*Sending me a secret message*

- (1) *Translate* secret message “The walk will be at 9am tomorrow” into a secret number by  $a \rightarrow 10, b \rightarrow 11, \dots, A \rightarrow 35, B \rightarrow 36, \dots$ :

$$W = 551714783210212078321821217811147810297871102278292422242727243273.$$

- (2) *Code*  $W$  by raising it to the power  $e$  and taking remainder mod  $n$ .

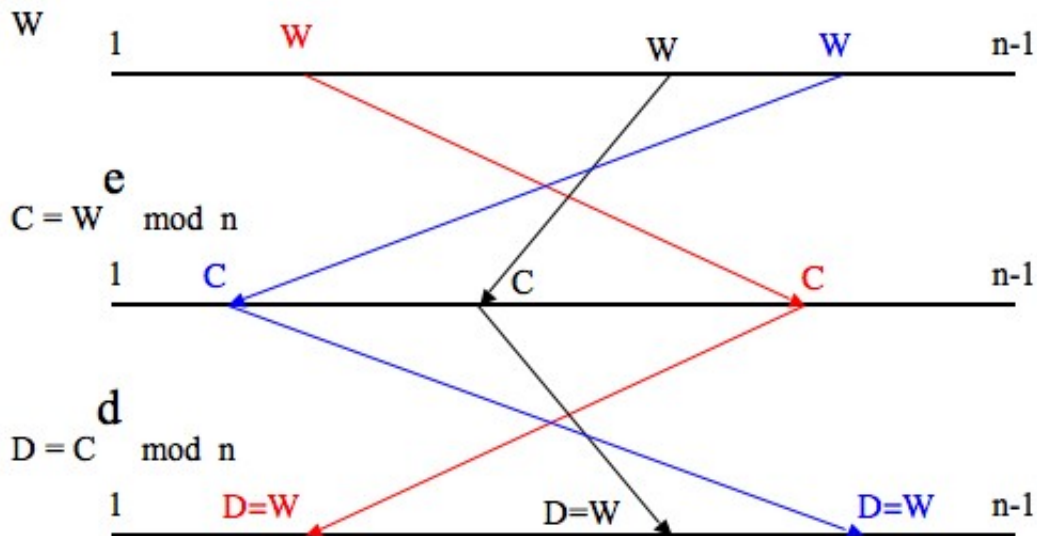
$$C = W^e \pmod n = 3130178295332760315857094698082641916093989301088502360650854635177956217466533375390945958659606911.$$

- (3) **FACT1:** For any  $e$  selected as before, i.e. relatively prime to  $m$ , the mapping

$$W \rightarrow C$$

is a “shuffle” (permutation) of  $\{1, 2, \dots, n - 1\}$ .

- (4) *Publish*  $C$  in the Canberra Times with a note that it is a coded secret message for me.



$W \rightarrow C$  is a shuffle (permutation) of  $\{1, \dots, n - 1\}$ .

*Decoding my secret message.* I do the following:

- (1) Decode  $C$  by raising it to the power  $d$  and taking remainder mod  $n$ .  
 $D = C^d \pmod n = 55171478321021207832182121781114781029787110227$   
 $8292422242727243273$ .

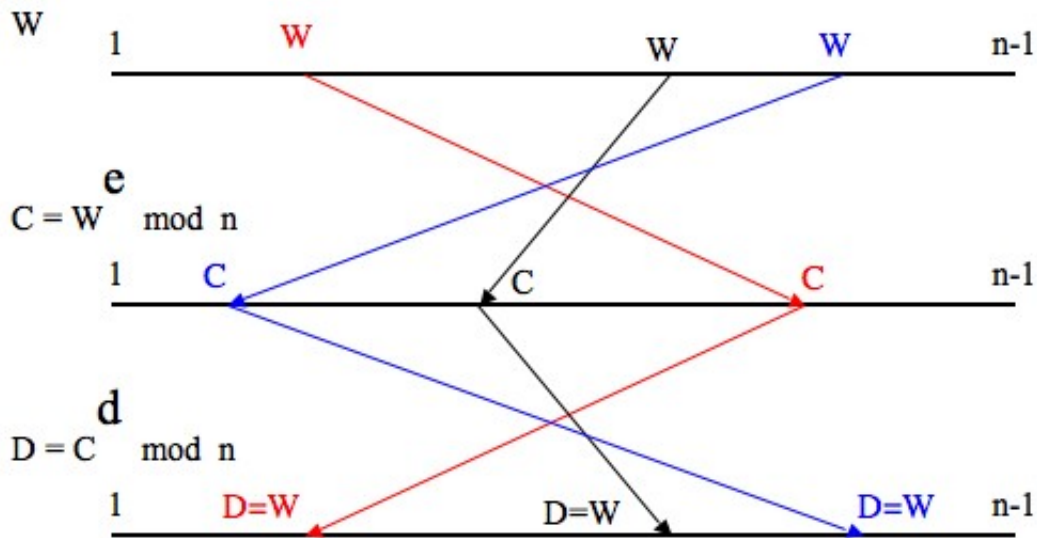
This is the same as  $W$ .

- (2) **FACT2:** For  $d$  selected as before, i.e. the inverse of  $e \pmod m$ , the mapping

$$C \rightarrow D$$

is an “unshuffle” (permutation) back to the original order  $\{1, 2, \dots, n-1\}$ .

- (3) Translate  $D (= W)$  back into the original secret message by  
 $10 \rightarrow a, 11 \rightarrow b, \dots, 35 \rightarrow A, 36 \rightarrow B, \dots$ :  
 “The walk will be at 9am tomorrow”



$C \rightarrow D$  is the “unshuffle” back to  $\{1, \dots, n-1\}$ .