RSA encryption

Why do we need to keep things secret?

- Historically, secret messages were used in wars and battles
  - For example, the Enigma cipher in WW2
- Computers are nowadays used to store lots of information about us
  - The recent "lost CDs in the post" contained data that was not kept secret
- Also need to make sure that online purchases are secure

Terminology

- Cryptography: study of creating secret codes
- Plaintext: the original message
- Ciphertext: the message after encryption
- Encryption: the process of creating a ciphertext
- Decryption: reversing encryption
- Cipher: name often given to an encryption

RSA

- The RSA cipher uses two keys and uses lots of Maths to make it work
- The key used for encryption is called the public key and the key used for decryption is called the private key (which is kept secret)
- To make it hard to break, one of the keys needs to be around 600 digits (2048 bits)
- Named after Rivest, Shamir and Adleman

RSA recipe

- Pick two large primes p and q
- Work out $n = p \times q$
- Work out $k = (p-1) \times (q-1)$
- Pick a public key e which does not have any factors (except 1) in common with k
- Find a private key d that $d \times e = 1 \pmod{k}$
- To encrypt m, work out $m^e \pmod{n}$
- To decrypt c, work out $c^d \pmod{n}$

Primes and Factoring

- For RSA, we have to pick two prime numbers, let's say p and q.
- Remember a prime number has exactly two factors (so 2 and 3 are prime, but not 1 or 4)
- We have to work out the product n of the two primes so $n = p \times q$
- To find p and q from n is hard – we would have to check all the (prime) numbers up to p or q. This is what makes RSA secure.

Modular Arithmetic

RSA encryption uses modular arithmetic.

We write $10 \pmod 6$

to mean "give me the remainder when 10 is divided by 6"

So $10 \pmod 6 = 4$ (because $10 = 6 \times 1 + 4$)

$75 \pmod 9 = 3$ ($75 = 9 \times 8 + 3$)

$56 \pmod{12} = 8$ ($56 = 12 \times 4 + 8$)

$89 \pmod{10} = 9$ ($89 = 10 \times 8 + 9$)

Keys

- We now pick a public key e
- We find a private key d such that:

  $d \times e = 1 \pmod{(p-1)(q-1)}$

  (There's a method called the extended Euclidean algorithm which can find this)
- To encrypt a number (message) M we do

  $M^e \pmod{n}$
- To decrypt, we do $C^d \pmod{n}$

Example

- Pick $p = 7$, $q = 13$ so $n = 7 \times 13 = 91$
- Pick $e = 5$ and then $d = 29$
  - Check $5 \times 29 = 145 = (2 \times 6 \times 12) + 1$
- To encrypt the number 10, we do

$$10^5 \pmod{91} = 10 \times 10 \times 10 \times 10 \times 10 \pmod{91} = 82$$

- To decrypt we do

$$82^{29} \pmod{91} = 10$$

Working out powers

We needed to work out 82^{29} (mod 91) – how can we do this quickly and easily?

We split up the power (29) as follows:

$82^{29} = 82^{1} \times 82^{4} \times 82^{8} \times 82^{16}$

and we work out these powers mod 91

Note that 82^{29} is quite big with 56 digits.

In Stages

$82^2 = 6724 = 81 \pmod{91}$

$82^4 = 82^2 \times 82^2 = 81 \times 81 = 9 \pmod{91}$

$82^8 = 82^4 \times 82^4 = 9 \times 9 = 81 \pmod{91}$

$82^{16} = 82^8 \times 82^8 = 81 \times 81 = 9 \pmod{91}$

$$\begin{aligned} \text{So, } 82^{29} &= 82 \times 9 \times 81 \times 9 \quad &\pmod{91} \\ &= 738 \times 729 &\pmod{91} \\ &= 10 \times 1 = 10 &\pmod{91} \end{aligned}$$

Using Letters

So far we've seen how to encrypt numbers. To encrypt text we give letter a value

A=1, B=2,…,Z=26 and Space=27

and then combine the numbers using Base 28.

Just as $234 = (2 \times 10^2) + (3 \times 10^1) + (4 \times 10^0)$

Then "BCD" $= (2 \times 28^2) + (3 \times 28^1) + (4 \times 28^0)$

$= 1568 + 84 + 4 = 1656$

Comments on RSA

- To make RSA fast we need to be able to find powers quickly – there are methods to help us do this
- The strength on RSA relies on the fact that it is generally hard to factor a very large number
- By using two keys, we can keep the private key secret
- There are many other "public key" methods