Public Key Cryptography

Traditional:
• Person A decides how they code the message.
• Person B needs to know how person A encoded the message.
  "code book".
• Person C can easily intercept this code book = read the message.

Want: a way to encode a message that doesn’t need a code book.
Idea: * B is going to provide in a very public way information (2 numbers).
* This information is enough for A to encode her message.
* B is going to withhold a critical piece of information that will allow B to decode.

Person C: all they can see is the public information - not enough to decode.
Steps:

B: 1) Pick two very large prime numbers, p and q.

2) Calculate: 
   \[ n := p \times q \]
   \[ b := (p-1) \times (q-1) \]

3) Pick a big number “a” that has no common factors with b.
   No numbers that divide both a and b (except 1).

4) Publish \((n, a)\).

A: 1) Convert your message into a string of numbers.

2) Split string of numbers into blocks of numbers which have less digits than digits of \(n\).
3) \( x = \) block of numbers.
   Calculate \( x^a \).

4) Divide \( x^a \) by \( n \).
   \[ x^a = kn + r \]
   remainder \( 0 \leq r < n \).

5) Send to B: \( r \).
Example

B: 1) \( p = 3 \quad q = 41 \).

2) \( n = p \times q = 3 \times 41 = 123 \)
\[
b = (p - 1) \times (q - 1) = 2 \times 40 = 80.
\]

3) Pick a number \( a \) with no common factors with \( b = 80 \).
\[
a = 27 = 3^3.
\]

Publish: \((n, a) = (123, 27)\).
Information that we've hidden: p and q.

A: \( x = 05 \) block that we want to encode.

Calculate \( x^2 = 5^{27} \)

divide by \( n = 123 \), \( r = 20 \).

Message that we send:

\( r = 20 \).

Q: How do we decode ??
Claim: Let $a$, $b$ be two numbers with no common factors. Then there exists two integers $s$ and $t$ such that:

$$as + bt = 1.$$ 

Check: $b = 80$, $a = 27$.

Want: $27s + 80t = 1$

Idea: Let's divide 80 by 27.

$$80 = 2 \times 27 + 26 \quad \Rightarrow \quad 26 = 80 + (-2) \times 27$$

$$27 = 1 \times 26 + 1$$

$$27 + (-1) \times 26 = 1$$
\[ 27 + (-1)(80 + (-2) \times 27) = 1 \]
\[ 27 + (-1) \times 80 + 2 \times 27 = 1 \]
\[ 3 \times 27 + (-1) \times 80 = 1 \]

**Want:** \( 27s + 80t = 1 \)

\[ s = 3 \quad \text{and} \quad t = -1 \]

**Euclidean Algorithm** \( \quad a < b \)

1. \( b = q_1 a + r_1 \quad 0 < r_1 < a \)
2. \( a = q_2 r_1 + r_2 \quad 0 < r_2 < r_1 \)
   \[ r_1 = q_3 r_2 + r_3 \quad 0 < r_3 < r_2 \]

If the remainder becomes 0, then \( \Rightarrow a \) and \( b \) have a common factor.
nth step \[ r_{n-2} = r_n r_{n-1} + 1 \]

* Work backwards until we get expression
      \[ 1 = a \cdot s + b \cdot t. \]

In our example: \( a = 27, \ b = 80. \)

Claim: \( s = \) key to enable us to decode the message.

\( \Rightarrow r^s \) divide by \( n \) take remainder remainder \( = x. \)
Example: $x = 05$ message before encryption.

$(n, a) = (123, 27)$.

Encrypt: $x^a = 5^{27}$

$\text{divide by }123=n$, and we got $r = 20$.

$r^s = r^3 = 20^3 = 8000$

$\text{divide by }n=123: \quad = 65 \times 123 + 5$

remainder $= 5$.

Why can’t Person C calculate the number $s$?
Key point: needed to know both 
\[ a = 27 \text{ and } b = 80 = (p-1)(q-1) \]

\[ \Rightarrow b \text{ was hidden.} \]

\((n, a)\) know: \(n\) is the product of \(p\) and \(q\).

Q: How do we find the prime \(p\) and \(q\)?

Very hard to factorise large numbers.

Largest publicly known factored \# was 
250 digits long 
(829 bits)

\(n\) less than 300 bits \(\leq 80\) digits 
- you can factor w/ a personal computer.
(n=pq, a)  a is relatively prime to b.

Q:  $x^a$ divided by $n$ $\Rightarrow$ $\Gamma$.
    $\Gamma^s$ divided by $n$ $\Rightarrow$ $X$.

\[
x^a = k\Gamma + \Gamma
\]
\[
\Gamma = x^a - k\Gamma
\]
\[\Gamma^s = (x^a - k\Gamma)(x^a - k\Gamma) \ldots (x^a - k\Gamma)
\]
\[= (x^a)^s + n(\text{bunch of stuff})
\]
\[= x^{as}
\]

as + bt = 1  from Euclidean Algorithm.

as = 1 - bt

as
\[ x^b = q^n + 1 \text{ for some } q. \]

Why is this true? 

\[ x^b = x \cdot (p-1)(q-1) = q^n + 1. \]

Thm (Euler's Thm): let \( n \) be any number.

Then \( a^{\varphi(n)} = q^n + 1 \)

\( \varphi(n) \) Euler's totient function \( \varphi(n) \) counts all the integers from 1 that are coprime with \( n \).
\( \varphi(n) \) counts all the numbers from 1 up to \( n \) that have no common factors with \( n \). (Includes 1).

E.g.: \( \varphi(5) = \#\{1, 2, 3, 4\} = 4 \)
\( \varphi(7) = \#\{1, 2, \ldots, 6\} = 6 \)
\( \varphi(p) = p - 1 \).

Challenge: \( \varphi(pq) = (p - 1)(q - 1) \) (check!).

\[ x^b - x^{(p-1)(q-1)} = qn + 1 \]
by above

\[ (x^b)^{-b} = (1 + qn)^{-b} \]
\[ = 1 + \sum_{\text{div by } n} \]

\[ = x \cdot x^{-b} + n \left( \text{bunch of stuff} \right) . \]
\[ = x \left( 1 + n\left( \ldots \right) \right) + n \left( \text{div by } n \right) \]
\[ = x + n\left( \ldots \right) \]
\[ = \text{just going to } x . \]