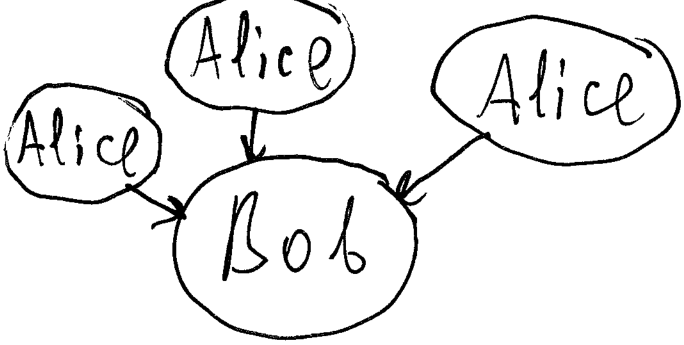
§11 RSA cryptosystem.

RSA comes from the names of the authors (Rivest, Shamir, Adleman).

It is an open key cryptosystem:



everyone can encrypt messages but only Bob can decrypt them.

Description of RSA cryptosystem:

Stage 1: Bob's set-up.

	Example
Choose two LARGE primes p, q, $p \neq q$	$p = 5$, $q = 11$
Compute $\underbrace{n = pq}_{\text{Modulus of RSA}}$, $\varphi(n) = (p-1)(q-1)$	$n = 55$ $\varphi(n) = 40$.
Choose an <u>encryption exponent</u> e with $\gcd(e, \varphi(n)) = 1$	$e = 7$
Compute the decryption exponent $d \equiv e^{-1} \pmod{\varphi(n)}$	$d = 23$ (check!)
Stage 2: Bob publishes the <u>public key</u> (n, e) but keeps $p, q, \varphi(n), d$ in secret.	Public key is $(55, 7)$.

Stage 3: Alice encodes the message, so it becomes the sequence $[m_1, m_2, \ldots, m_\ell]$ where $m_i \in \underbrace{\{0, 1, 2, \ldots, n-1\}}_{\text{alphabet}}$.

$[2, 3]$.

Stage 4: Alice encrypts the message by replacing each m_i by $m_i^e \pmod{n} \equiv m_i'$ to get $[m_1', m_2', \ldots, m_\ell']$.

$2^7 \equiv 18 \pmod{55}$
$3^7 \equiv 42 \pmod{55}$
Encrypted message is $[18, 42]$.

Stage 5: Alice sends $[m_1', m_2', \ldots, m_\ell']$ to Bob.

Stage 6: Bob decrypts the message by replacinge each m_i' by $(m_i')^d \pmod{n}$.

$18^{23} \equiv 2 \pmod{55}$
$42^{23} \equiv 3 \pmod{55}$

Check that it works: we need to check that $(m_i')^d \equiv m_i \pmod{n}$

Indeed $(m_i')^d \equiv (m_i^e)^d \equiv m_i^{ed} \pmod{n}$ and

$ed \equiv 1 \pmod{\varphi(n)} \Rightarrow ed = k\varphi(n) + 1$

Finally, $m_i^{ed} \equiv m_i^{k\varphi(n)+1} \equiv$ [RSA theorem] $\equiv m_i \pmod{n}$.

Check the security of the method. If someone else wants to decrypt the message, they:

(a) Need to compute d given (n, e), but not p, q or $\varphi(n)$.

It is believed (not formally proved) that this requires:

(b) Computation of $\varphi(n)$ given n (and the fact that it is a product of two primes)

That is equivalent to finding p, q.

Indeed if p, q are known then

$$\varphi(n) = \varphi(pq) = (p-1)(q-1)$$

If we know $\varphi(n)$ then we know:

$$pq = n$$

Also $\varphi(n) = (p-1)(q-1) = pq - (p+q) + 1$

$$\Rightarrow p+q = n - \varphi(n) + 1$$

Then p, q are solutions of quadratic equation:

$$x^2 - (n - \varphi(n) + 1)x + n = 0$$

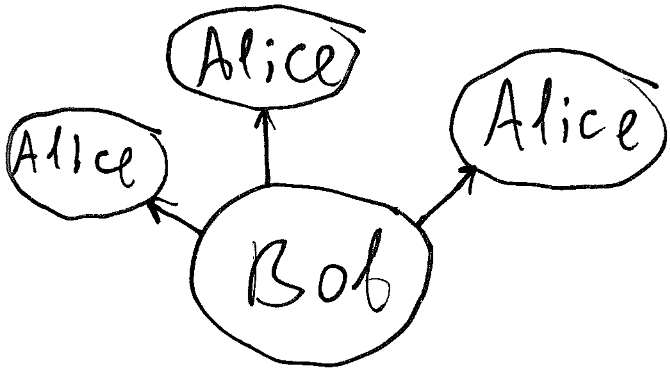
(requires computation of square roots).

Therefore to ~~go~~ decrypt the message we need to:

(c) Factorize a huge n as a product of primes.

So for RSA to be secure, p and q should be very large ($n \sim 2048$ bits).

§ 11.2 Digital signatures with help of RSA.



Only Bob can encrypt the message and everyone can decrypt it.

In this case Bob encrypts the message $[m_1, m_2, \ldots, m_l]$ by replacing each m_i with $m_i^d \pmod{n} \equiv m_i'$.

Alice decrypts the message by replacing each m_i' with $(m_i')^e \pmod{n}$.