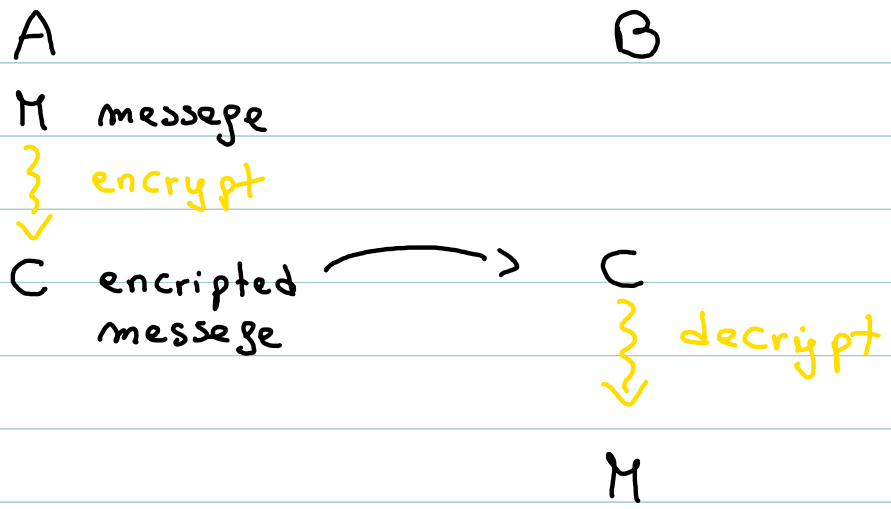
Lesson 27

RSA algorithm

Goal Send a secret message



RSA encryption/decryption method

Done by B

1. Choose primes p, q (we want p and q to be more than 100 digits long).

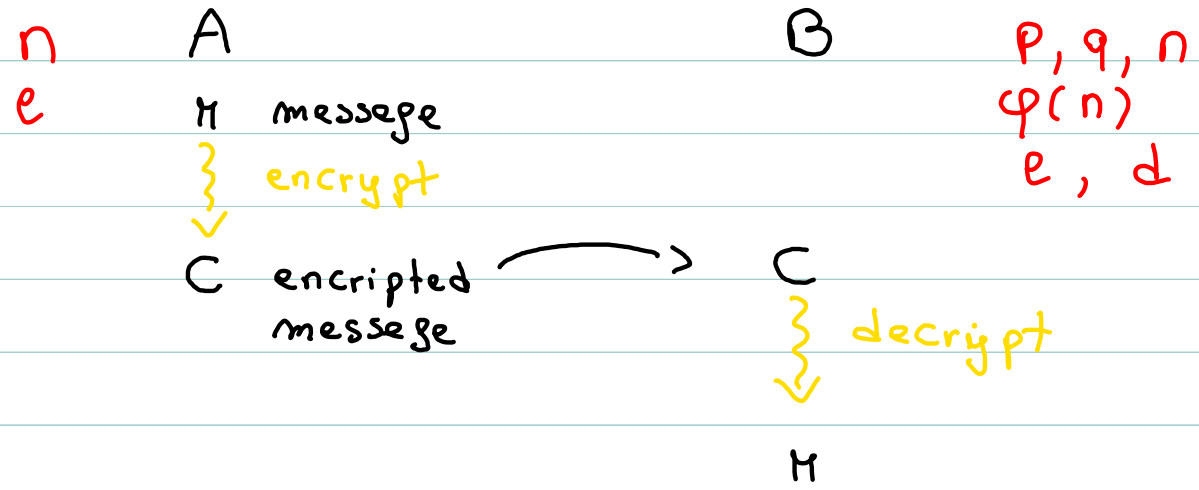
2. Compute $n = pq$

3. Compute $\phi(n) = (p-1)(q-1)$

4. Choose e relatively prime to (p-1)(q-1)

5. Solve $e \cdot x \equiv 1 \bmod \phi(n)$. Call the solution d.

6. Publish n, e, keep everything else secret.


n
e
A
M message
encrypt
C encripted message
B
C
decrypt
M
p, q, n
φ(n)
e, d

$C = M^e \bmod n$

Encryption of P M

Compute $C = M^e$ mod n

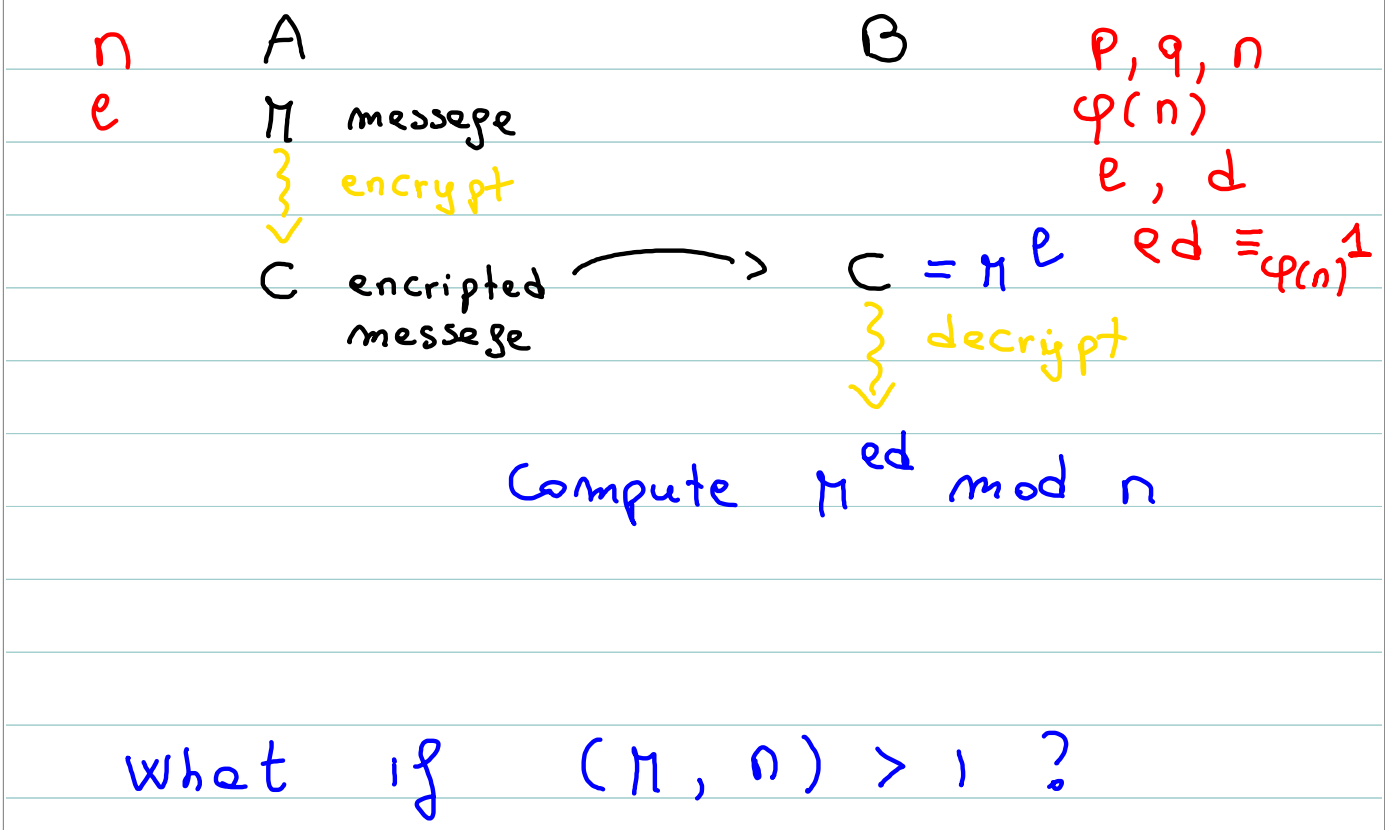
Decryption of C

Receive $C = M^e$ compute $C^d = M^{ed} \equiv M$ mod n

ed= 1+k ϕ (n) therefore

$M^{ed} = M^{1+k\phi} = M \cdot (M^{\phi(n)})^k \equiv M$ mod n

by Euler's theorem .


n
e
A
M
message
encrypt
C
encripted
message
B
C = M^e
decrypt
p, q, n
φ(n)
e, d
ed ≡ 1 (mod φ(n))
Compute M^ed mod n

what if $(M, n) > 1$?

what if $\gcd(M, n) > 1$? $n = p \cdot q$

p q distinct primes. Recall $de = 1 + k\varphi(n)$; $\varphi(n) = (p-1)(q-1)$

Claim $M^{de} \equiv M \bmod n = pq$

1) $M^{de} \equiv M \bmod p$ since if $(M, p) > 1$ then both M^{de} and M are congruous to 0 mod p and if $(M, p) = 1$, we have

$M^{de} = M^{1+k(p-1)(q-1)} = M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 \bmod p$

2) Similarly $M^{de} \equiv M \bmod q$

3) so p div $M^{de} - M$, q div $M^{de} - M$ therefore

$M^{de} - M = pk = qh$ for some $h, k \in \mathbb{Z}$

p div qh $(p, q) = 1$ so p div h,

therefore $M^{de} - M = q \underbrace{p \cdot s}_{h}$ for some $s \in \mathbb{Z}$

and $M^{de} \equiv M \bmod qp = n$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

$n = 4867$
$e = 851$

$p = 31$, $q = 157$
$\varphi(n) = 30 \cdot 156 = 4680$
$d = 11$

you send BYE

$11\ 34\ 14 \rightsquigarrow 11^{851}_{34}\ 14^{851}$ mod 4867

$851 = 512 + 256 + 64 + 16 + 2 + 1$

$113^2 \equiv 3035$
$113^4 = (3035)^2 \equiv 2861$
$113^8 \equiv (2861)^2 \equiv 3896$
$113^{16} \equiv 2531$
$113^{32} \equiv 989$
$113^{64} \equiv 4721$
$113^{128} \equiv 1848$
$113^{256} \equiv 3337$
$113^{512} \equiv 4740$

ALL COMPUTATION MOD 4867

$113^{851} \bmod 4867 \equiv \boxed{1774}$

Now compute $414^{851} \mod 4867$
$= 3000$

you send 1774 3000

Receiver computes $1774^{11} \mod 4867$
$3000^{11} \mod 4867$

Retrieves 113414

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

$n = 4187$

$e = 851$

$p = 31$, $q = 157$

$\varphi(n) = 30 \cdot 156 = 4680$

$d = 11$

My message to you

3338 (1), 3976 (2), 637 (3), 427 (4), 1979 (5), 4733 (6), 136 (7), 2671 (8)