RSA

- Rivest Shamir Adelman 1977
- Clifford Cocks @ GHCQ, 1973 → (kept mode public in 1997)

Security

- one-way function
- Easy to mult. two large primes
  - ↳ but no known general way to factor in reasonable time

Ex $2^{2^{20}} + 1$ has 315,653 digits
- known to be compound
- factors are unknown

KeyGen

① Choose p, q primes of several hundred digits

② $n = pq$

③ Choose e S.T.

(A) $\gcd(e, (p-1)(q-1)) = 1$

(B) $e < n$

Recall Extended Euclid:

Let a, b be integers with at least 1 of a, b non-zero

Then $\exists$ integers d, t

s.t.

$ad + bt = \gcd(a, b)$

$= 1$ if a, b relatively prime

So, [illegible]

Since

$\gcd(e, (p-1)(q-1)) = 1$

$ed + (p-1)(q-1)T = 1$

$ed - 1 = -T \cdot (p-1)(q-1)$

$ed \equiv 1 \mod (p-1)(q-1)$

$d \equiv e^{-1} \mod (p-1)(q-1)$

Public key: n, e

private key: d

pting
} middle
} much
, bignum

ENC

① break msg into blocks
s.t. len(block) < n
(on each block)

② Let m be one such block

$$enc(m) = c \equiv m^e \bmod n$$

Public key
n, e

Dec

claim

$$Dec(c) = m \equiv c^d \bmod n$$

private key
d

Bob sends message to Alice using Alice's Public key n, e

Alice
↳ knows
p, q, n, e
↳ computes $d \equiv e^{-1} \bmod (p-1)(q-1)$
↳ private key

Bob
↳ knows
n, e Alice's public key
m, $enc(m) = c \equiv m^e \bmod n$

intrude

Proof

Two possibilities for m

① $\gcd(p, m) = \gcd(q, m) = 1$

② m is a multiple of either p or q

m is NOT a multiple of both p and q

↯ $m < n$ by assumption

Suppose m is a multiple of both p and q

$p \mid m$ and $q \mid m$

m may be written as a product of primes

$m = f_1 f_2 \cdots f_k$

Since $p \mid m$ and p is prime

$p =$ one of the factors, say f_p

Some can be called f_q, ... f_k

So $m = f_1 \cdots f_p \cdots f_q \cdots f_k$

clearly $pq \mid m$

$m = pqR = nR$

but this is impossible b.c. $m < n$

So m is NOT a multiple of <u>both</u> p and q

BACK TO 2 Cases

① $\gcd(p,m) = \gcd(q,m) = 1$

$enc(m) = c \equiv m^e \bmod n$

$c^d \equiv m^{ed} \bmod n$

Recall

$ed \equiv 1 \bmod (p-1)(q-1)$

Skip [$e = d^{-1}$ DO and $d = e^{-1}$

$ed - 1 = k(p-1)(q-1)$ do / q Cmq.

$ed = k(p-1)(q-1) + 1$

$m^{ed} = m^{k(p-1)(q-1)+1}$

$= m\, m^{k\phi(p)\phi(q)}$

Since p, q are prime

$\phi(n) = \phi(pq)$

$= \phi(p)\phi(q)$

$m^{ed} = m\, m^{k\phi(n)}$

Recall Euler

if $\gcd(a,n) = 1$

$$a^{\phi(n)} \equiv 1 \bmod n$$

Since $\gcd(m,p) = \gcd(m,q)$ by assumption

$\gcd(m,n) = 1$ Since $n = pq$

$$m^{\phi(n)} \equiv 1 \bmod n$$

and

$$m^{k\phi(n)} \equiv 1^k \bmod n$$

$$\equiv 1 \bmod n$$

$$m\, m^{k\phi(n)} \equiv m \bmod n$$

Since $m^{ed} = m\, m^{k\phi(n)}$

$$m^{ed} \equiv m \bmod n$$

but $c \equiv m^e \bmod n$

$$c^d \equiv m^{ed} \bmod n$$

$$m \equiv c^d \bmod n$$

QQ Claimed

Case 2

m is a multiple of either p or q but not both

Choose p

Let $m = kp$

$m \equiv 0 \mod p$ Def of Congruence OR ASSUMPTION $m - 0 = kp$

Since

$$c \equiv m^e \mod n$$

$$c^d \equiv m^{ed} \mod n$$

Since

$m \equiv 0 \mod p$

$m^{ed} \equiv 0 \mod p$

$m \equiv m^{ed} \mod p$ Eq 1

Recall

$$ed = -T(p-1)(q-1) + 1$$

Let $k = -T$

$$ed = k(p-1)(q-1) + 1$$

$$m^{ed} = m^{k(p-1)(q-1)+1}$$

$$= m\, m^{k(p-1)(q-1)}$$

$$\equiv m\, m^{k\phi(q)\phi(p)} \mod q$$

By assumption $\gcd(m, q) = 1$

By Euler $m^{\phi(q)} \equiv 1 \mod q$

So $m^{ed} \equiv m\, m^{(\phi(q))^{k\phi(p)}} \mod q$

$\equiv m \mod q$ eq. 2

Recall Eq 1: $m \equiv m^{ed} \mod p$

Putting it together

$$m^{ed} \equiv m \mod p$$

$$\underline{m^{ed}} \equiv \underline{m} \mod q$$

This system of linear eqns. has a solution mod pq by the Chinese remainder theorem

$$m^{ed} \equiv m \mod pq$$

$$\equiv m \mod n$$

March 3
Start w/ Format
Reduction formula p.48

but $c \equiv m^e \bmod n$ by enc

so $c^d \equiv m^{ed} \equiv m \bmod n$

since $m < n$

so $m \equiv m^{ed} \equiv c^d \bmod n$

RSA in a nutshell

Parameters

p, q both large primes

$n = pq$

① keygen

choose e s.t.

$e < n$

$\gcd(e, (p-1)(q-1))$

$= \gcd(e, \phi(p)\phi(q))$

$= \gcd(e, \phi(n)) = 1$

Public key: (n, e)

Private key: d s.t.

$d \equiv e^{-1} \bmod (p-1)(q-1)$

② Encrypt

m is message

$len(m) < n$

$c = m^e \pmod n$

③ Decrypt

$m = c^d \pmod n$

Security

d can't be found from e, n

To find d Requires

$\phi(pq) = (p-1)(q-1)$

b.c $d \equiv e^{-1} \bmod (p-1)(q-1)$

the factorization of n

Ex (with small numbers)

$p = 37$
$q = 43$

$n = pq = 1591$

choose e s.t. $e < n$ and
$\gcd(e, (p-1)(q-1)) = 1$

$(37-1)(43-1) = 1512$

Let $e = 17$

$d \equiv e^{-1} \bmod 1512$

~~$e^{\phi(n)-1} \equiv e^{-1} \bmod 1512$~~

~~$\phi(1512) = \text{euler\_phi}(1512) = 432$~~

~~$e^{431} \equiv e^{-1} \bmod 1512$~~

~~$d = 17^{431} \equiv 17^{-1} \bmod 1512$~~

$17^{-1} = \text{inverse\_mod}(17, 1512) = 89$

$d = 17^{-1} \equiv 89 \bmod 1512$

Public Key = $(n, e) = (1512, 17)$
private key = $d = 89$

Let $M = 285|628|101|73$

Divide into 4 blocks

$m_1 = 285\ 628\ 101\ 73$

$m_1 = 285$

$m_2 = 628$

$m_3 = 101$

$m_4 = 73$

$C = Enc(m) = m^e \bmod n$

Enc (Store these in Base

$C_1 = enc(m_1) = 285^{17} \bmod 1591$

$= 935$

$C_2 = 628^{17} \bmod 1591$

$= 665$

$C_3 = 101^{17} \bmod 1591$

$= 1158$

$C_4 = 73^{17} \bmod 1591$

$= 406$

$M = Dec(C) = C^d \bmod n$

$m_1 = 935^{89} \bmod 1591$

$= 285$

$m_2 = 665^{89} \bmod 1591$

$= 628$

$m_3 = (1158)^{89} \mod 1591$
$= 101$

$m_4 = (406)^{89} \mod 1591$
$= 73$

RSA Details

Choose e To be Small
3, 17, 65537 work

All are of form 2^n+1

Notice $2^1+1 = 3$
$2^2+1 = 5$
$2^3+1 = 9$
$2^4+1 = 17$
$\vdots$
$2^{16}+1 = 65537$

$010+1 \rightarrow 011$
$100+1 \rightarrow 101$
$1000+1 \rightarrow 1001$
$10000+1 \rightarrow 10001$

$1000\ldots0001$ (15 zeros)

Makes Modulo exponentiation easier

if q is an integer

$$a^q = a^{q \pmod{p-1}} \pmod{p}$$

Fermat Reduction Formula

Fermat

if p is prime & a

$a^{p-1} \equiv 1 \pmod{p}$

Pf

Let

$q = (p-1)\ell + r$ by DA

$q - r = (p-1)(p-1)^{\ell-1} r$

$r \equiv q \pmod{(p-1)}$

Let q be an integer

$a^q = a^{(p-1)\ell + r}$

$a^q = a^{(p-1)\ell} \cdot a^r \pmod{p}$

By Fermat

$a^{p-1} \equiv 1 \pmod{p}$

$a^q \equiv a^r \pmod{p}$

$a^q = a^{q \pmod{p-1}} \pmod{p}$

Ex $p=B$ $a=10$ $q=17$

$10^{27} \equiv (10^{12})^2 10^3 \mod 13$

by $10^{12} \equiv 1 \mod 13$ by Fermat

so $10^{27} \equiv 10^3 \mod 13$

By the reduction Formula

$10^{27} \equiv 10^{27 \mod 12} \mod 13$

$\equiv 10^3 \mod 13$

RSA Attacks

1. Digital Signature Attack
   - Will await study of Dig. Signature
2. Common modulus
3. Low e attack
4. Timing

1, 2, 3 are protocol attacks

Common modulus

- Scene
  - -- Difficult to find large primes
  - -- You reuse them

Alice and Bob both encrypt same msg

$$C_1 \equiv m^{e_1} \bmod n$$

$$C_2 \equiv m^{e_2} \bmod n$$

Eve has e_1, e_2, n the public keys

C_1, C_2 b.c. she intercepts

Suppose e_1, e_2 are relatively prime

by Extended Euclid

$\exists\ s, t$ s.t.

$se_1 + te_2 = 1$

one of s and t will be negative

$$\left[\begin{array}{l} ab + cd = 1 \\ ab = 1 - cd \end{array}\right] \text{ey}$$

Suppose $s < 0$

$$\left[\text{Enc}(m) = m^e = c\right] \pmod{pq}$$

$$\left((c_1)^{-1}\right)^{-s} (c_2)^t \equiv m^{e_1 s} m^{e_2 t} \pmod{n}$$

$$\equiv m^{e_1 s + e_2 t} \pmod{n}$$

$$\equiv m \pmod{n}$$

note: necessary that $\gcd(c, n) = 1$ for c_1^{-1} to exist

Ex $p = 37 \quad q = 43 \quad n = 1591$

$m = 500 \quad e_1 = 17 \quad e_2 = 5$

$c_1 \equiv 500^{17} \mod 1591 = 849$

power.mod(500, 17, 1591) = 849

$c_2 \equiv 500^{5} \mod 1591 = 22$

$17s + 5t = 1$

xgcd(17, 5) = (1, −2, 7)

$\left(\left(849^{-1}\right)^{-1}\right)^{-(-2)} \cdot (22)^{7} \mod 1591$

$849^{2} \cdot 22^{7} \mod 1591$

$= 500$

Factoring

(1) Conjecture:
no way to recover d w/out factoring pq
has never been proven

(2) Rabin Cipher
Proven that recovering key is as hard as factoring

insecure against Chosen CT

Factoring Techniques

(A) Trial Division

if n is composite it must have a factor c s.t. $c \leq \sqrt{n}$

Divide n by all k

$$2 \leq k < \lfloor \sqrt{n} \rfloor$$

Requires $\sqrt{n}$ divisions which grow in complexity

look at links for RSA challenge

(B) Fermat's method

(Burton p. 87, McAndrew p. 25)

Let $n = pq$ where p and q are prime

Claim: $p+q$ is even, $p-q$ is even

pf p is odd, q is odd

$\Rightarrow$ $p = s+1$, $q = t+1$ } where s, t are even

$$p+q = (s+1) + (t+1)$$
$$= (s+t) + 2$$

Which is even

Similarly for $p-q$ is even is

so

$p+q = 2r$ | b.c. both are even
$p-q = 2k$ |

$$\begin{array}{r} p+q = 2r \\ + \; p-q = 2k \\ \hline 2p = 2(r+k) \\ p = r+k \end{array}$$

$$\begin{array}{r} p+q = 2r \\ -(p-q = 2k) \\ \hline 2q = 2r-2k \\ q = r-k \end{array}$$

$$n = pq$$
$$= (r+k)(r-k)$$
$$= r^2 - k^2$$

$$n + k^2 = r^2$$

① Add squares to n until a square is found

② Factors of n: $r \pm k$

Ex $n = 5609$

k	$k+n^2$	n^2
1	5610	—
2	5613	—
3	5618	—
4	5625	75

Polard Rho

Begin w/ Def.

Def.

Congruence class

A Congruence is the set of all integers that have the same remainder when divided by n

Notated

$[3]_5$ is the set of all integers that have the remainder 3 when divided by 5

$[3]_5 : \{\ldots, 3, 8, 13, 18, \ldots\}$

These are integers, m, s.t.

$m - 3 = k \cdot 5 \quad \forall k \in \mathbb{Z}$

$3 - 3 = 0 \cdot 5$

$8 - 3 = 1 \cdot 5$

$13 - 3 = 2 \cdot 5$

⋮

Using Set builder notation

$$[3]_5 = \{3 + 5k \mid k \in \mathbb{Z}\}$$

how many congruence classes mod 5

Exactly 5

$$[0]_5, [1]_5, \ldots, [5-1]_5$$

Now imagine n, known to be composite

it has n congruence classes

$$[0]_n, [1]_n, \ldots, [n-1]_n$$

Generate a pseudo-random seq

① Let $f(x) = x^2 + a \quad a \neq 0, -2$

② generate

$x_1, x_2, x_3, \ldots$

$$x_{k+1} \equiv f(k) \pmod{n} \quad k = 0, 1, 2, \ldots$$

beginning with x_0

$$x_1 = f(x_0)$$
$$x_2 = f(f(x_0))$$
$$\vdots$$

Suppose d is a non-trivial divisor of n not small compared with $\sqrt{n}$

There will probably be

x_j, x_k that belong to the same cong. class mod d but a different class mod n

that is

$$x_k \equiv x_j \bmod d$$

$$x_k \not\equiv x_j \bmod n$$

Then

$$d \mid (x_k - x_j)$$

but $n \nmid (x_k - x_j)$

$\Rightarrow \gcd(x_k - x_j, n)$ is a non trivial divisor of n, namely d

Now: d is not known in advance

For each x_k x_j

for $j < k$ $(x_k - x_j)$

compute $\gcd(x_j, x_k)$

Ex $n = 2189$

$f(x) = x^2 + 1$

$x_0 = 1$

$x_1 = 1+1 = 2$

$x_2 = 4+1 = 5$

$x_3 = 25+1 = 26$

$x_4 = 676+1 = 677$

$x_5 = (677)^2 + 1 \pmod{2189} = 829$

$\gcd((5-1), 2189) = 1$

$\gcd((26-2), 2189) = 1$

$\gcd((677-5), 2189) = 1$

$\gcd((829-26), 2189)) = 11$

$\gcd(45$

$\text{and } 11 * 199 = 2189$

Computationally expensive: ~~[illegible]~~

$\gcd(x_k - x_j, n)$ for each $j < n$

Trick: Reduce gcds by
(1) not using every j
(2) Relying on repetitions in the modulus seq.

Instead only look at cases $k = 2j$

Let d be some undiscovered non-trivial divisor of n

if $x_k \equiv x_j \pmod d$ with $j < k$

Then by the way in which x is selected

$$\underbrace{x_{j+1}}_{\text{by def } f} = \underbrace{f(x_j)}_{\text{by assumption}} \equiv f(x_k) = \underbrace{x_{k+1}}_{\text{By def.}} \pmod d$$

When the seq $\{x_k\}$ is reduced mod d, a block, q $k-j$ integers is repeated

because this is the period

~~if they repeat, the residues will repeat, too~~

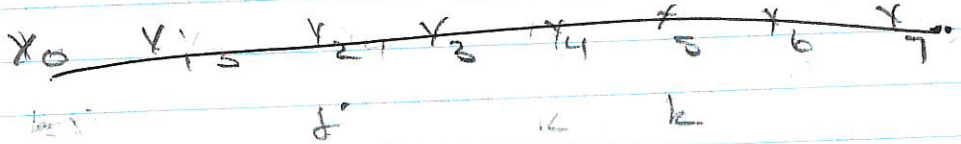
if $r \equiv s \pmod{k-j}$, $r \geq j$, $s \leq j$

then $x_r \equiv x_s \bmod d$

and $x_n \equiv x_T$ when T is a multiple q^{k-j} larger than j

Somewhere in one of those repeating seq. there will probably exist integer

$$1 < \gcd(x_{2k} - x_k, n) < n$$



~~$2 \equiv 5 \bmod (k-2)$~~

3

Ex

$n = 30623$

$x_0 = 3$

$f(x) = x^2 - 1$

x_9 x_{10}

358193475 1283025655325756 24

integer Seq:

3, 8, 63, 3968, 4801, 21104, 28526, 18819, 18926

x_0 x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8

$x_2 - x_1 = 63 - 8 = 55$ $\gcd(55, n) = 1$

$x_4 - x_2 = 4801 - 63 = 4738$ $\gcd(4738, n) = 1$

$x_6 - x_3 = 28526 - 3968 = 24558$ $\gcd(24558, n) = 1$

$x_8 - x_4 = 18926 - 4801 = 14125$ $\gcd(14125, n) = 113$

$x_{10} - x_5$

Notice, when original list is reduced mod 113, we get

x_0 x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 x_9 x_{10}

3, 8, 63, 13, 65, 86, 50, 13, 65, 86, 50

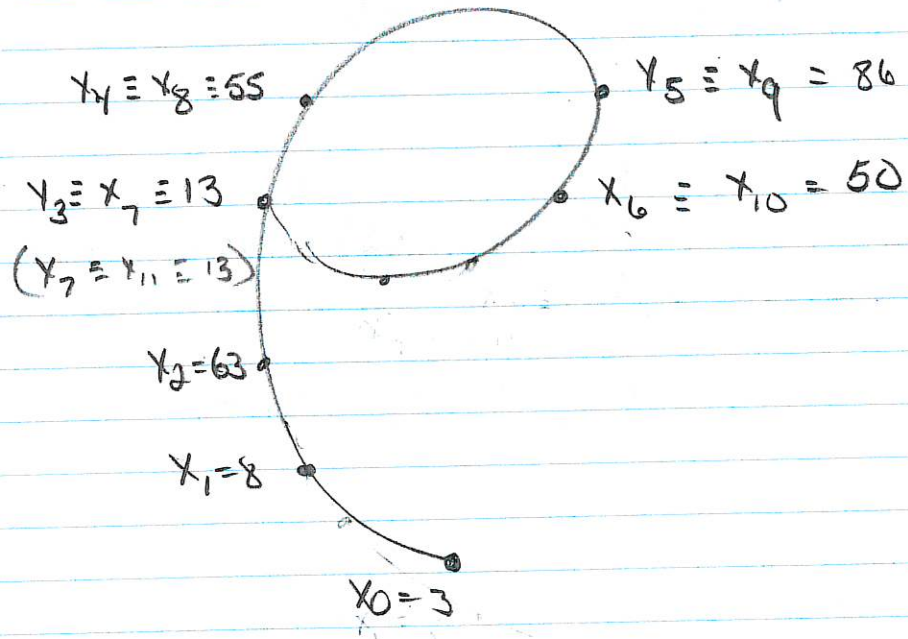
Periodic

$3 \equiv 7 \pmod 4$

$13 \equiv 13 \pmod{113}$

$x_{2r} \equiv x_r \pmod{113}$ $x_8 \equiv x_4 \pmod{113}$ period = 4

This produces



$X_0 = 3$

$$F_n = 2^{2^n} + 1$$

$$F_8 = 2^{256} = pq$$

Pollard Rho. this

$p = 1,238,926,361,552,897$

unable to determine q