FACTORING

GOAL. FIND A FACTOR OF A NUMBER N

WE ASSUME $N < 2^m$, SO IT'S A m-BIT NUMBER

THE ALGORITHM

1) SELECT NUMBER $a < N$

$$\underset{\downarrow}{\text{CONTINUE}} \xleftarrow{\text{NO}} \boxed{GCD(a,N)=1} \xrightarrow{\text{YES}} \text{DONE}$$

SIDE NOTE : GCD IS EASY AND FAST

EUCLIDIAN ALGORITHM

$a = 1071 \qquad b = 462$

$1071 = q_0 \cdot \underline{462} + r_0 \qquad q_0 = 2 \quad r_0 = \underline{147}$

$462 = q_1 \cdot \underline{147} + r_1 \qquad q_1 = 3 \quad r_1 = \underline{21}$

$147 = q_2 \cdot \underline{21} + r_2 \qquad q_2 = 7 \quad \boxed{r_2 = 0}$

$GCD(1071, 462) = 21$

FAST SINCE IT REQUIRES $O([\log N]^3)$ OPERATIONS

SIDE NOTE:

NUMBERS $a < N$ COPRIME TO N (I.E. $GCD(a, N) = 1$) FORM A FINITE GROUP UNDER MULTIPLICATION MOD N.

INDEED: IF A AND B DONT SHARE A FACTOR WITH N SO DOES THEIR PRODUCT.

WHAT ABOUT INVERSION?

LET $U_N = \{ a < N : GCD(a, N) = 1 \}$

NOW LET'S CONSIDER MAP

$$a \mapsto ab \pmod N$$

TAKE $b, b' < N$ AND SUPPOSE

$$ab \equiv ab' \pmod N$$

$$\Downarrow$$

$$N \mid ab - ab' = a(b - b')$$

SINCE $a \in U_N$

$$N \mid b - b'$$

BUT $b, b' < N$ THEN

$$b = b' \quad \text{(WITHOUT MOD)}$$

THUS IF $ab \equiv ab' \pmod N$ => $b = b'$

MAP IS INJECTIVE

SO IT TAKES FOR EACH b IT TAES DIFFERENT VALUE

SINCE WE HAVE $N-1$ DIFFERENT b

AND $N-1$ DIFFERENT VALUES OF THE MAPPING

THE MAPPING IS SURJECTIVE => BIJECTVE

THUS THERE EXIST b SUCH THAT

$$ab \equiv 1 \pmod N$$

AND b IS a^{-1} ■

IF WE HAVE AN FINITE GROUP WE CAN DEFINE AN „ORDER" r TO BE THE SMALEST POSTIVE INTIGER TO SATISFY

$$a^r \equiv 1 \pmod N$$

HAS TO EXIST SINCE EXP FINALLY LAND ON THE SAME NUMBER IN FINTE GROUP

COMMENT : IN GENERA r IS VERY LARGE

FINDING ORDER r IS THE PERIOD FINDING PROBLEM OF THE FUNCTION

$$\boxed{f_{N,a}(x) = a^x \pmod N}$$

BUT WE CAN ALREADY DO IT FAST!

SHORT COMMENT ON EFFICIENT CALCULATIONS OF $f_{N,a}(\cdot)$

LET $x = x_{m-1} 2^{m-1} + x_{m-2} 2^{m-2} + \dots + x_0$ (BINARY)

$$\Downarrow$$

$$a^x \pmod N = \left(a^{2^{m-1}}\right)^{x_{m-1}} \left(a^{2^{m-2}}\right)^{x_{m-2}} \cdots (a)^{x_0} \pmod N$$

BUT

$$a^{2^j} \pmod N = \left(a^{2^{j-1}}\right)^2 \pmod N$$

SO NEXT EXPONENT IS SQUARE OF THE PREVIOUS ONE

WE NEED ONLY $m-1$ (CLASSICAL) mod N MULTIPLICATIONS

SUPPOSE WE HAVE FOUND PERIOD r

NEXT WE NOTICE THAT IF r IS EVEN

$$N \mid (a^{\frac{r}{2}}+1)(a^{\frac{r}{2}}-1)$$

·) $a^{\frac{r}{2}}-1$ CANNOT DIVIDE N SINCE THE ORDER IS r AND NOT $r/2$; IF IT DOES THEN THE REAL ORER IS OF THE ORDER $\frac{r}{2}$.

·) IF $a^{\frac{r}{2}}+1 \mid N$ THEN WE RESTART THE ALGORITHM SINCE IT WILL GIVE US ONLY TRIVIAL DIVIDORS (1 AND N)

WE LOOK FOR CASES WHERE

$$a^{\frac{r}{2}}+1 \nmid N \quad \text{OR} \quad a^{\frac{r}{2}} \neq -1 \pmod N$$

BECAUSE THEN $a^{\frac{r}{2}}+1$ AND N

<u>SHARE THE COMMON FACTOR</u>

THEREFORE

$$GCD(a^{\frac{r}{2}}+1, N) \neq 1$$

IS A FACTOR!

SO NOW WE CHECK HOW LIKELY IS TO FIND APPROPRIATE r. (SINCE THIS SCENARIO IS NOT PERFECT AND REQUIRES REPETITIONS)

ASIDE: CHINESE REMINDER THEOREM:

LET'S SUPPOSE

$$N = p_1 \cdot p_2 \qquad p_1 \neq p_2$$

WHICH IS THE HARDEST POSSIBLE CASE TO FACTOR

WE HAVE THAT FOR EACH $a < N$

THERE EXIST UNIQUE $a_1 < p_1$ AND $a_2 < p_2$

SUCH THAT

$$a \equiv a_1 \pmod{p_1}$$

$$a \equiv a_2 \pmod{p_2}$$

PROOF:

1) UNIQUENESS:

LET $a \equiv a_1 \pmod{p_1}$ AND $a \equiv a_2 \pmod{p_2}$

ALSO $b \equiv a_1 \pmod{p_1}$ AND $b \equiv a_2 \pmod{p_2}$

IT MEANS THAT $a \equiv b \pmod{p_1}$ AND $a \equiv b \pmod{p_2}$

SINCE p_1, p_2 ARE COPRIMES

$$p_1 \mid a-b \quad \text{AND} \quad p_2 \mid a-b \Rightarrow p_1 \cdot p_2 \mid a-b$$

SO $N \mid a-b$ AND SINCE $a<N$ AND $b<N$

THEN $\underbrace{a=b}$

2) EXISTANCE:

CONSIDER A MAP

$$\Phi : \{0,1,\dots,N-1\} \to \{0,\dots,p_1-1\} \times \{0,\dots,p_2-1\}$$

$$\Phi : a \longmapsto (a \bmod p_1 ,\ a \bmod p_2)$$

WE SHOWED THAT THIS MAP IS INJECTIVE

$$\Phi(a) = \Phi(b) \Rightarrow a=b$$

BUT DOMAIN AND CO DOMAIN ARE EQUAL SIZES (N)

SO THIS MAP IS A BIJECTION

EVERY PAIR (a_1, a_2) HAS SOME

PREIMAGE a

$\blacksquare$

NOW USING CHINESE REMINDER THEOREM WE CAN „SPLIT" OUR SEARCH:

$$a^r \equiv 1 \pmod{p_1 p_2} \Rightarrow \begin{cases} a_1^r \equiv 1 \pmod{p_1} \\ a_2^r \equiv 1 \pmod{p_2} \end{cases}$$

WHERE

periods of each "split"

$$\underline{r = LCM(r_1, r_2)}$$

SO IF EITHER r_1 OR r_2 IS EVEN WE ARE STILL IN A GAME. NOW WE HAVE 4 SCENARIOS

$$\begin{cases} a^{\frac{r}{2}} \equiv -1 \pmod{p_1} \\ a^{\frac{r}{2}} \equiv -1 \pmod{p_2} \end{cases} \quad \begin{cases} a^{\frac{r}{2}} \equiv -1 \pmod{p_1} \\ a^{\frac{r}{2}} \equiv 1 \pmod{p_2} \end{cases} \quad \begin{cases} a^{\frac{r}{2}} \equiv 1 \pmod{p_1} \\ a^{\frac{r}{2}} \equiv -1 \pmod{p_2} \end{cases} \quad \begin{cases} a^{\frac{r}{2}} \equiv 1 \pmod{p_1} \\ a^{\frac{r}{2}} \equiv 1 \pmod{p_2} \end{cases}$$

$$\downarrow$$

$$\begin{cases} a^{\frac{r}{2}} + 1 = q_1 p_1 \\ a^{\frac{r}{2}} + 1 = q_2 p_2 \end{cases}$$

$$\downarrow$$

co prime !

$$a^{\frac{r}{2}} + 1 = q_3 \cdot p_1 \cdot p_2$$

$$\downarrow$$

$$a^{\frac{r}{2}} \equiv -1 \pmod{N}$$

FAIL

START OVER

$$\begin{cases} a^{\frac{r}{2}} + 1 = q_1 p_1 \\ a^{\frac{r}{2}} + 1 = q_2 p_2 + 2 \end{cases}$$

$$a^{\frac{r}{2}} + 1 \neq q_3 p_1 \cdot p_2 \quad \checkmark$$

FOUND NON TRIVIAL DIVISOR

$$\downarrow$$

$$\begin{cases} a^{\frac{r}{2}} - 1 = q_1 p_1 \\ a^{\frac{r}{2}} - 1 = q_2 p_2 \end{cases}$$

$$a^{\frac{r}{2}} - 1 = q_3 p_1 p_2$$

$$a^{\frac{r}{2}} \equiv 1 \mod p_1 p_2$$

$$\downarrow$$

FAIL

we found shorter period

SUPPOSE

$$r_1 = 2^{c_1} \cdot k_1$$

$$r_2 = 2^{c_2} \cdot k_2$$

k_1, k ARE ODD

$\cdot)\quad c_1 > c_2 \quad \Rightarrow \quad r = LCM(r_1, r_2) = 2^{c_1} \cdot k_3$

$k_3 = LCM(k_1, k_2)$

$\tilde{k}_1 \cdot k_1 = k_3$

$\tilde{k}_2 \cdot k_2 = k_3$

1) $r = 2 \cdot r_2 \cdot \tilde{k}_2$

$\downarrow$

$\underline{a^{\frac{r}{2}} = a^{r_2 \cdot \tilde{k}_2} \equiv 1 \pmod{p_2}}$

$\downarrow$

$$\begin{cases} a \equiv a_1 \pmod{p_1} \\ a^{r_1} \equiv a_1^{r_1} \pmod{p_1} \equiv 1 \pmod{p_1} \\ a^{r_2} \equiv a_2^{r_2} \pmod{p_2} \equiv 1 \pmod{p_2} \end{cases}$$

2) $r = r_1 \cdot \tilde{k}_1$

$\downarrow$

$\underline{a^{\frac{r}{2}} = a^{\frac{r_1}{2} \tilde{k}_1} \equiv -1 \pmod{p_1}}$

$\downarrow$

$a^{r_1} \equiv 1 \pmod{p_1}$

$\sqrt{a^{r_1}} \equiv \pm 1 \pmod{p_1}$

we choose -1 since $+1$ gives us contradiction with r_1 being shortest period

<u>WE WIN!</u>

IN THIS SCENARIO WE SATISY EQ FROM THE PREVIOUS PAGE AND WE FOUND A DIVISOR.

$\cdot)\quad c_1 < c_2 \quad \Rightarrow$ WE <u>ALSO WIN</u> (ANALOGOUS ARGUMENT)

$\cdot)\quad c_1 = c_2 \quad \Rightarrow \quad r = r_1 \cdot \tilde{k}_1 = r_2 \cdot \tilde{k}_2$ AND

$a^{\frac{r}{2}} \equiv -1 \pmod{p_1}$ AND $a^{r/2} \equiv -1 \pmod{p_2}$

<u>WE LOOSE!</u>

SO THE PROBLEM BOILS DOWN TO FINDIING HOW PROBABLE IT IS TO $c_1 \neq c_2$, CAUSE THEN WE WIN.

ASIDE:

MULTIPLICATIVE GROUP MOD p IS CYCLIC SO THERE IS „PRIMITIVE" ELEMENT SO THAT POWERS OF THIS ELEMENT ARE ALL ELEMENTS OF THE GROUP

order of this primitive

$$G_p^\times \text{ - GROUP} \Rightarrow \exists g \in G_p^\times : \quad G_p^\times = \{g, g^2, \dots, \underbrace{g^{\underline{p-1}}}_{\equiv\, 1 \pmod p}\}$$

WITHOUT PROOF, BUT RATHER SIMPLE

KEEP INMIND THAT THE GROUP IS FINITE

OK, SO THERE IS THIS PRIMITIVE IN A GROUP WITH ORDER $p-1$. WHAT ~~IS~~ ARE THE ORDERS OF OTHER ELEMENTS?

b	$p-1$
b^2	$\begin{cases} \frac{p-1}{2} & \text{iff } 2 \mid p-1 \\ p-1 & \text{iff } 2 \nmid p-1 \end{cases}$
b^3	$\begin{cases} \frac{p-1}{3} & \text{iff } 3 \mid p-1 \\ p-1 & \text{iff } 3 \nmid p-1 \end{cases}$

hardest case!

LET'S SAY $p-1 = 2^1 \cdot k$ $\quad k \in$ odd

THEN ORDER

- EVEN POWER : k
- ODD POWER : $2 \cdot k$

SO IN GENERAL WE CAN WRITE AN ORDER FOR EACH ELEMENT AS

$$\underbrace{r = 2^{c} \cdot (\text{odd})} \qquad c \in \{\overset{\text{even power}}{0}, \overset{\text{odd power}}{1}\}$$

IN THIS WORST CASE SCENARIO THE ODDS OF CHOSING TWO DIFFERENT PARITIES OF THE ORDER IS $\boxed{\frac{1}{2}}$

c_2 \ c_1	0	1
0	✗	✓
1	✓	✗

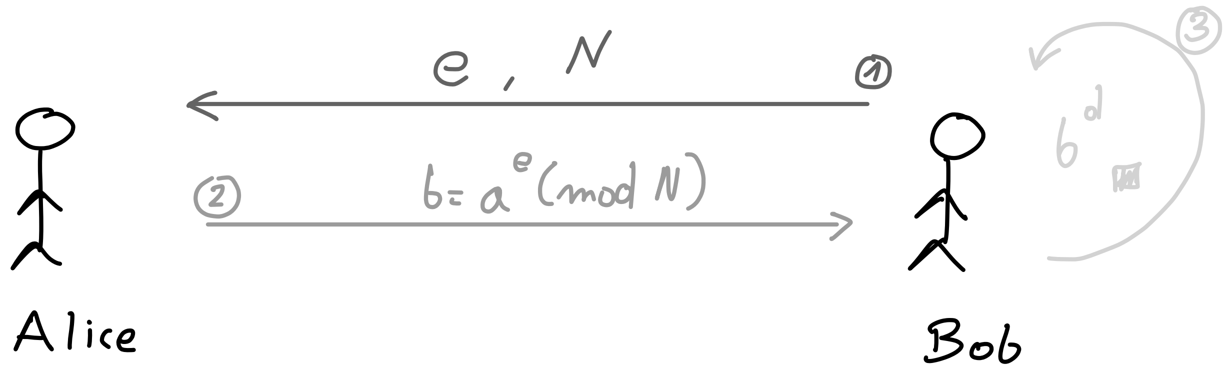
IF WE HAVE BIGGER POWERS OF TWO THEN THE PROBABILITY TO NOT BE EQUAL GROWS.

REMEMBER THAT WE HAVE CHOSEN FOR $N = p_1 p_2$. IF WE HAVE MORE PRIMES IT ONLY GROWS!

RSA

PUBLIC CRYPTOGRAMY IS IMORTANT WHEN WE NEED TO COMMUNICATE THROUGH AN INSECURE CHANNEL LIKE INTERNET.

LET'S CONSIDER THE FOLLOWING ALGORITHM:



a

$b = a^e \pmod{N}$

p, q $\quad N = p \cdot q$

$e < \varphi(N)$

$d = e^{-1} \mod \varphi(N)$

1) BOB CHOSES TWO BIG PRIMES p AND q WHICH ARE SECRET. HE COMPUTES

$$N = p \cdot q$$

2) HE ALSO CALCULATES EULER FUNCTION

$$\varphi(N) = N - p - q + 1 = (p-1)(q-1)$$

WHICH IS A NUMBER OF NUMBERS LESS THAN N THAT ARE COPRIME WITH N

SO FOR SUCH NUMBER WE HAVE N NUMBERS IN TOTAL MINUS ALL MULTIPLIES OF p AND q (+1 because we do not remove N itself)

$\varphi(N)$ IS

- EASY WHEN KNOWING p AND q
- HARD WHEN KNOWING ONLY N

3) BOB PSEUDO-RANDOMLY SELECTS $e < \varphi(N)$ THAT IS COPRIME WITH $\varphi(N)$

4) BOB SENDS TO ALICE (AND EVERYONE ELSE) VALUE OF $\underline{e}$ AND $\underline{N}$

5) ALICE WANTS TO SEND SECRET NUMBER $a < N$

SHE ENCODES IT BY COMPUTING:

$$b = f(a) = a^e \pmod N$$

AND SENDS TO BOB

{ fast because repeating squaring

WE ASSUME a COPRIME WITH N

VERY LIKELY !?

6) BOB DECODES :

·) FROM EULER'S THEOREM

$$a^{\varphi(N)} \equiv 1 \pmod N$$

SHORT PROOF:

NUMBER THAT ARE COPRIME TO N AND LESS THAN N FOR A GROUP OF ORDER $\varphi(N)$. WE CHOSE RANDOM ELEMENT a IN THE GROUP AND EXPONENT IT UNITIL WE GET BACK a. THOSE ELEMENTS FORM A GROUP WITH ORDER k SUCH THAT

$$a^k \equiv 1 \pmod N$$

BUT LAGERANGE THEOREM SAYS

$$\underset{\text{subgroup}}{k} \mid \underset{\text{group}}{\varphi(N)}$$

SO $\varphi(N) = M \cdot k$

SO $$a^{\varphi(N)} = (a^k)^M \equiv 1^M = 1 \pmod N$$

■

•) SINCE $GCD(e, \varphi(N)) = 1$ → it is in a group!

WE KNOW THAT e HAS INVERSE

$$d \equiv e^{-1} \pmod{\varphi(N)}$$

$$\Updownarrow$$

$$ed \equiv 1 \pmod{\varphi(N)}$$

BOB CALCULATES d

HOW TO CALCULATE d?

BY PRODUCT OF EUCLIDIAN ALGORITHM

OF CALC. $GCD(e, \varphi(N)) = 1$

CHAIN OF REMINDERS:

$$1 = R_n$$

$$R_n = R_{n-2} - q_{n-1} R_{n-1}$$

$$R_{n-1} = R_{n-3} - q_{n-2} R_{n-2}$$

$$\vdots$$

REWRITING

$$1 = (1 + q_{n-1} q_{n-2}) R_{n-2} - q_{n-1} R_{n-3}$$

$$1 = (-q_{n-1} - q_{n-3} (1 + q_{n-1} q_{n-2})) R_{n-3} +$$
$$+ (1 + q_{n-1} q_{n-2}) R_{n-4}$$

$$\vdots$$

SO WE CAN EXPRESS 1 AS A LINEAR COMBINATION OF ANY TWO SUCCESIVE REMINDERS

EVENTUALLY ON THE TOP WE GET

$$1 = d \cdot e + q \cdot \varphi(N)$$

THIS IS WHAT WE LOOK FOR !

∎

·) BOB DECODES

$$f^{-1}(b) = b^d \pmod N = a^{ed} \pmod N$$

$$= a^{1 + \varphi(N) \cdot k} \pmod N =$$

using $a^{\varphi(N)} \equiv 1 \pmod N$

$$= a \pmod N$$

∎

SO BOB HAS SUCESFULLY DECODED

A MESSAGE.

COMMENTS

) IF EVE HAS SUPER FAST FACTORING MACHINE

THIS SCHEME IS INSECURE.

1) FACTOR N : p, q

2) COMPUTE $\varphi(N)$

3) COMPUTE $d = e^{-1} \pmod{\varphi(N)}$

↳ THEN SHE CAN DECODE

.) WE NEED LESS THAN THAT !

WE JUST NEED

ORDER MODULO N OF ENCODED ~~MESSAGE~~ MESSAGE $a^e \pmod N$

WHY ?

SINCE e AND $\varphi(N)$ ARE COPRIME

THEN ORDER OF $a^e \pmod N$ IS THE

SAME AS ORDER OF a.

ONCE WE KNOW $\overset{\text{ORDER}}{\text{Ord}(a)}$

BYPRODUCT OF $GCD(e, \text{Ord}(a))$

EVE COMPUTES $\tilde{d} : \tilde{d} e \equiv 1 \pmod{\text{Ord}(a)}$

THEN

$$(a^e)^{\tilde{d}} \equiv a \cdot \left(a^{\text{Ord}(a)}\right)^{\text{integer}} \pmod N \equiv a \pmod N$$

decrypted

THE ONLY GUARANTEE FOR THIS TO WORK IS OUR ASSUMPTION THAT IT'S HARD TO FACTOR NUMBERS!