(Fermat - Euler Theorem) Let p be a prime.

Let $a \not\equiv 0 \pmod{p}$. Then

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

—

We can use this to test whether a number is prime or not.

Suppose we want to test if n is Prime. If we can find some $a \not\equiv 0 \pmod{n}$ and $a^{n-1} \not\equiv 1 \bmod n$, then we know n is not prime.

Defn: We say a witnesses nonprimality of n.

Example: $n = 91$

$$2^{90} = (2^{10})^9$$

$$= (1024)^9$$

$$\equiv (23)^9 \pmod{91}$$

$$\equiv 64 \pmod{91}$$

(I used a Calculator!)

$$3^{90} \equiv ? \pmod{91}$$

Pingala's algorithm

$3^{666} \bmod 667$

Idea is to keep track of exponents!

Half (666

333

−1 (332

166

83

82

41

40

20

10

660

(285)3 = 188

285

187

13(3) = 39

13

(393)(3) ≡ 512

393

547

(243)(243) ≡ 353

5

4

2

1

243

81

9

3

This test doesn't always work!

Defn: (CARMICHAEL NUMBER)

A Composite number n which satisfies

$GCD(a, n) = 1 \Rightarrow a^{n-1} \equiv 1 \pmod{n}$

Ex: 41041 is a Carmichael number.

41041 Divisible by 11

$41041 = 11 \times 3731$

$= 11 \times 7 \times 533$

$$= 11 \times 7 \times 13 \times 41$$

$$(a, 41041) = 1 \iff (a,7) = (a,11)$$

$$= (a,13) = (a,41) = 1.$$

$$a^6 \equiv 1 \pmod 7 \Rightarrow a^{41040} \equiv 1 \pmod 7$$

$$a^{10} \equiv 1 \pmod{11} \Rightarrow a^{41040} \equiv 1 \pmod{11}$$

$$a^{12} \equiv 1 \pmod{13} \Rightarrow a^{41040} \equiv 1 \pmod{13}$$

$$a^{40} \equiv 1 \pmod{41} \Rightarrow a^{41040} \equiv 1 \pmod{41}$$

So, $\boxed{a^{41040} \equiv 1 \pmod{41}}$

—

Every prime factor p of n satisfies $p-1 \mid n-1$.

—

So we need another test!

Let p be a prime number. Then

$$x^2 \equiv 1 \pmod{p} \iff x \equiv \pm 1 \pmod{p}$$

($\Leftarrow$:) If $x \equiv \pm 1 \pmod{p}$

then $x^2 \equiv 1 \pmod{p}$

($\Rightarrow$:) If $x^2 \equiv 1 \pmod{p} \Rightarrow (x^2 - 1) \equiv 0 \pmod{p}$

$\Rightarrow (x-1)(x+1) \equiv 0 \pmod{p}$

$\Rightarrow x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$

$$27182^2 \equiv 1 \pmod{41041}$$

↓

not ± 1

So 41041 is not prime.

(Miller Rabin primality test)

For $N < 25\,326\,001$ and N composite either 2, 3 or 5 will work.

Primitive roots

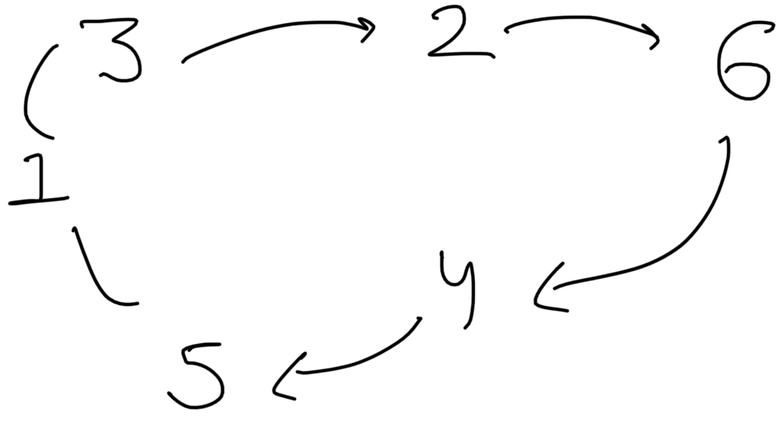
Given n and a such that $GCD(a,n)=1$

we say a is primitive root if

multiplication by $a \bmod n$ yields a

single cycle of length $\phi(n)$.

Example: Mod 7



Thm: If n is prime, then there exists a primitive root.

Lemma: Let λ be a positive integer. Then the number of elements of $\phi(p)$ of cycle-length λ is either 0 or $\phi(\lambda)$.

Pf: Suppose it is not 0.

Let a be an element with cycle length λ.

Look at a^e for $0 \le e \le \lambda - 1$

$$(a^e)^\lambda = (a^\lambda)^e \equiv 1 \pmod{p}$$

How many of these have cycle length λ?

Cycle length of $a^e = \dfrac{\lambda}{\gcd(e, \lambda)}$

(Why?)

Cycle length of a^e is $\lambda \iff \gcd(e, \lambda) = 1$

Lemma: (Totient sum formula)

Let N be a positive integer. Then

$$\sum_{d \mid N} \phi(d) = N$$

Example: $N = 6$

$$\phi(1) + \phi(2) + \phi(3) + \phi(6)$$

$$= 1 + 1 + 2 + 2 = 6$$

We will prove this lemma by showing a bijection between two sets.

$$\left\{ \frac{1}{N}, \frac{2}{N}, \frac{3}{N}, \dots, \frac{N-1}{N}, \frac{N}{N} \right\} = S_1$$

$$\left\{ \frac{a}{d} \;\middle|\; \begin{array}{c} \gcd(a,d) = 1 \\ d \mid N \quad 1 \le a \le d \end{array} \right\} = S_2$$

$$\# S_1 = \# S_2$$

$$\# S_1 = N \qquad \# S_2 = \sum_{d \mid N} \phi(d)$$

Let's prove what we wanted to prove.

Thm: If n is prime, then there exists a primitive root modulo n.

Pf: Suppose not.

If $a^l \equiv 1 \pmod{p}$ then $l \mid p-1$ & $l \neq p-1$.

For every divisor d of $p-1$, there are either 0 or $\phi(d)$ elements of length d.

$$(0 \text{ or } \phi(r_1)) + \cdots + (0 \text{ or } \phi(r_k))$$

r_i are divisors of $p-1$

$= p-1$

$$= \sum_{d \mid p-1} \phi(d)$$

They must be same !

Example:

mod 7

$3, 3^2, 3^3, 3^4, 3^5, 3^6$

↓ Primitive

↓ primitive

$\phi(6) = 2$

Towards Chinese Remainder Theorem

Motivation: Studying System of Congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

Qn: Does this system has a Solution? If yes, how many?

$$X \equiv 3 \pmod{12}$$

$$X \equiv 1 \pmod{15}$$

$$X \equiv 1 \pmod{9}$$

What about this one ?

$$X \equiv 1 \pmod{15}$$

$$X \equiv 1 \pmod{9}$$

$$X \equiv a_1 \pmod{n_1}$$

$$\vdots$$

$$X \equiv a_r \pmod{n_r}$$

——— *

(CRT) Assume n_i are pairwise coprime i.e, $\gcd(n_i, n_j) = 1$ for $i \neq j$

then there exists a unique solution to (*) (written above) mod N

where $N = n_1 n_2 \cdots n_r$

$$x \equiv 1 \pmod{15}$$

$$\Longleftrightarrow \quad x \equiv 1 \pmod{3}$$
$$x \equiv 1 \pmod{5}$$

$$x \equiv 1 \pmod{9}$$

$$\left.\begin{aligned} x &\equiv 1 \pmod{5} \\ x &\equiv 1 \pmod{9} \end{aligned}\right\} \Rightarrow \boxed{x \equiv 1 \pmod{45}}$$

Example 2

$$x \equiv 2 \pmod 5$$

$$x \equiv 1 \pmod 3$$

$$x \equiv a_1 \pmod{n_1} \qquad \gcd(n_1, n_2) = 1$$

$$x \equiv a_2 \pmod{n_2}$$

$$1 = m_1 n_1 + m_2 n_2$$

Take $x = a_2 m_1 n_1 + a_1 m_2 n_2$

$$x \equiv a_1 m_2 n_2 \pmod{n_1}$$

$$\equiv a_1 (1 - m_1 n_1) \pmod{n_1}$$

$$\equiv a_1 \pmod{n_1}$$

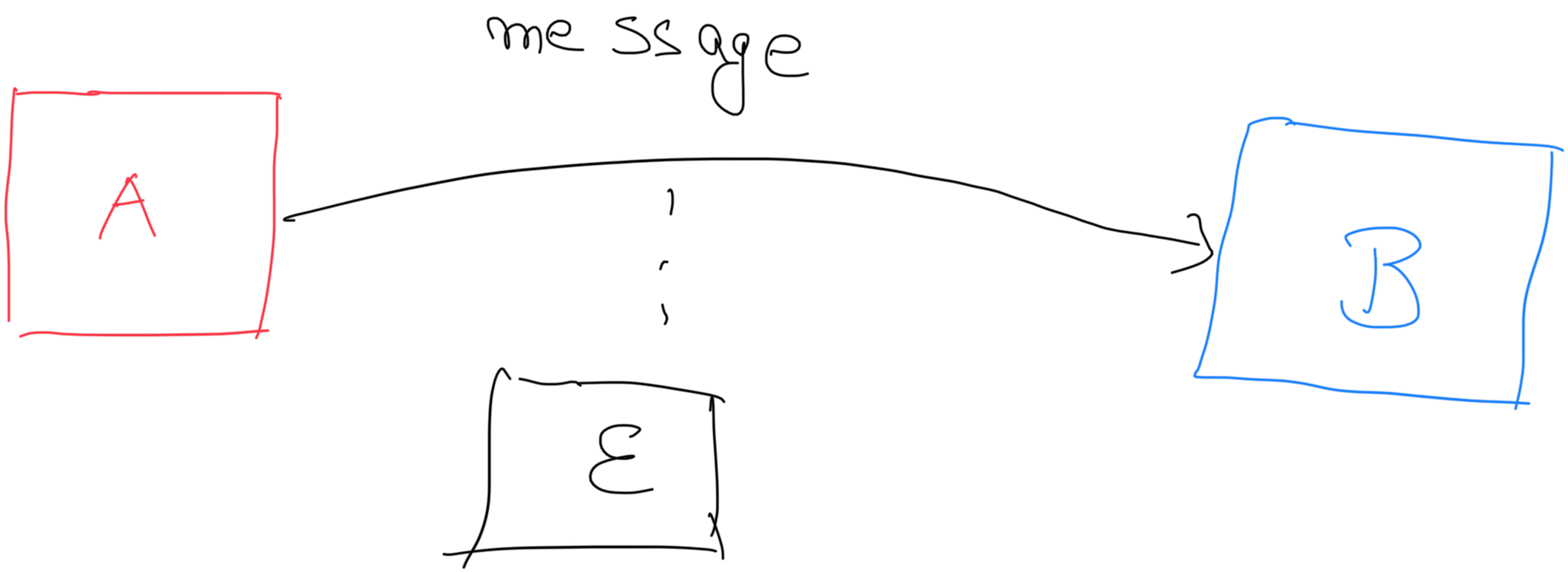
Uniqueness:

$$x_1 \equiv x_2 \pmod{n_1}$$

$$x_1 \equiv x_2 \pmod{n_2}$$

$$\Leftrightarrow \quad x_1 \equiv x_2 \pmod{n_1 n_2}$$

Applications : Cryptography



Idea is to prevent eavesdropping!

Basic Cipher:

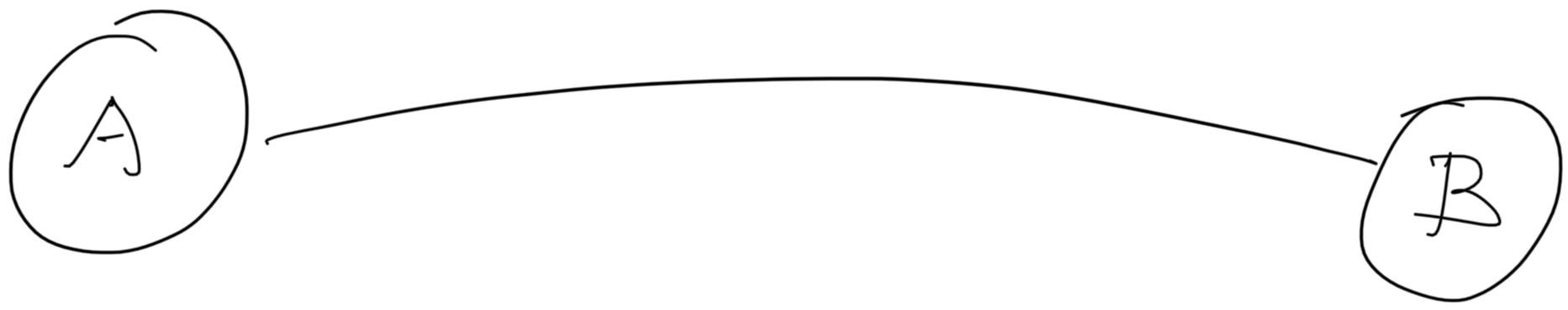
Original message: MEET ME AT GOLD CAFE.

↓ +3 ALPHABETS

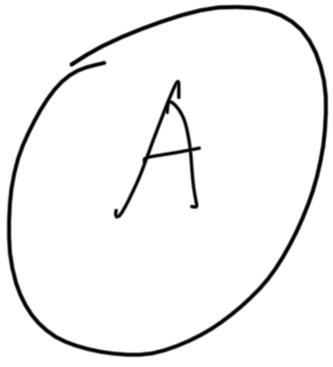
Encrypted message: PHHW PH DW JROG FDIH.

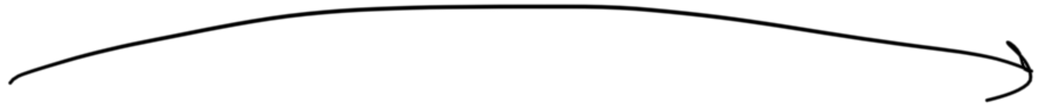
We need Some thing that is hard to break!

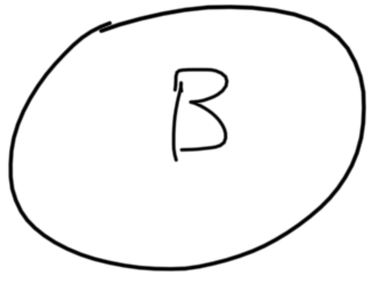
DIFFIE - HELLMAN PROTOCOL



(1) A chooses a prime p and a primitive root g modulo p.
(p should be large enough.)







(P, g)

(P, g)

For g (997, 7)

(997, 7)

---

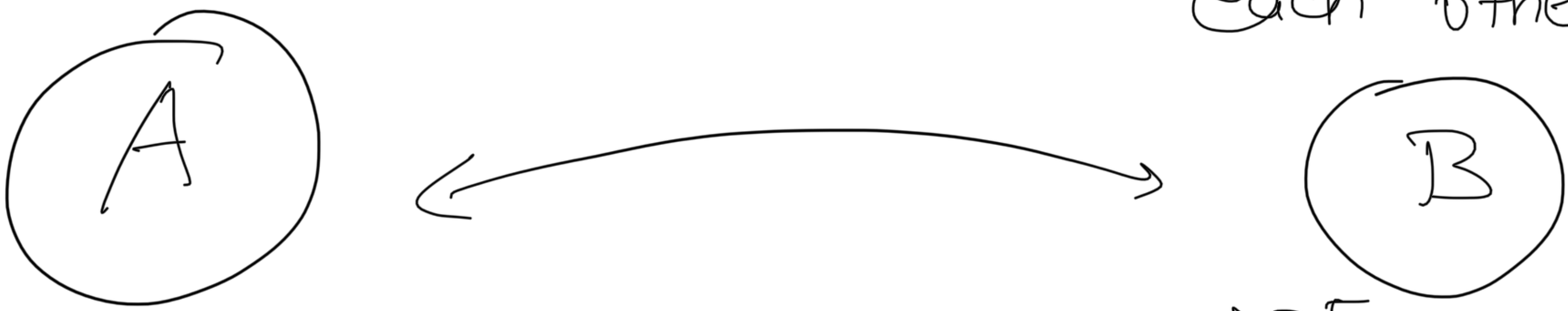
(2) Secret information

a = 36

b = 125

(3) A Computes g^a

B Computes g^b & Share with each other.



$7^{36} \equiv 729 \bmod 997$

$7^{425} \equiv 616 \pmod{997}$

(4) A computes $(g^b)^a$ & don't Share!

B Computes $(g^a)^b$

This secret key can be used as a cipher in their future communications.

Even if someone listens,

$$\underbrace{P, g, g^a}_{C}, g^b$$

To find a or b we need to solve

$$g^a \equiv c \pmod{p}$$ for a

Discrete logarithm problem is hard to Solve!

RSA

Rivest Shamir Adleman (1978)

(1) Alice chooses two prime numbers p, q say $p = 89$ (Secret)
$q = 103$

$N = pq$ and e (say 13) are made public.

(2) Bob wants to send a message

m, computes $C = m^e \pmod N$

and sends to Alice.

$C = m^e \pmod N$

(3) Alice Computes $\phi(N) = \phi(P)\,\phi(Q)$

$= (P-1)(Q-1)$

d s.t $de \equiv 1 \pmod{\phi(N)}$

$(m^e)^d = (m)^{ed} = m^{\phi(N)x+1}$

$\equiv m \pmod{N}$

↓

Recovers message m.