Recap:

Euler's Theorem:

$$a^{\phi(n)} \equiv 1 \mod n \quad , \quad \gcd(a,n) = 1 \quad , n \geq 2$$

Req.

e.g. $20 = 2^2 \cdot 5$

$\phi(20) = (2^2 - 2^1)(5^1 - 5^0)$

$= 2 \cdot 4 = \underline{\underline{8}}$

Fermat's Little Theorem:

If $n = p$ s.t. $p$ is prime:

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

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

Use to find Inverse:

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

$$a \cdot \underbrace{a^{\Phi(n)-1}}_{a^{-1}} \equiv 1 \mod n \quad , \quad \boxed{a^{-1} \equiv a^{\Phi(n)-1} \mod n}$$

In $n = p$ s.t $p$ is prime:

$$\boxed{a^{-1} \equiv a^{p-2} \mod p}$$

## To calculate exponents:

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

$$a^{k\cdot\phi(n)+c} \equiv \left(a^{\phi(n)}\right)^k \cdot a^c \mod n$$

$$= 1^k \cdot a^c \mod n$$

e.g.

$$3^{257} \mod 11 \equiv 3^{25\cdot 10+7} = 3^7 \mod 11$$

$$\equiv 3^3 \cdot 3^3 \cdot 3 = 5 \cdot 5 \cdot 3 = \underline{\underline{9}}$$

## Calculate exponents:

1) "Easy" case: use $a^{k\cdot(p-1)+c} \bmod p \equiv a^c \bmod p$
2) "Medium" case: use $a^{k\cdot\varphi(n)+c} \bmod n = a^c \bmod n$
3) Use square multiply:
   1) Convert exponent to Bits
   2) If bit is 1, square and multiply
      else square
   3) MSB kicks off algorithm.

# Public Key Cryptography:

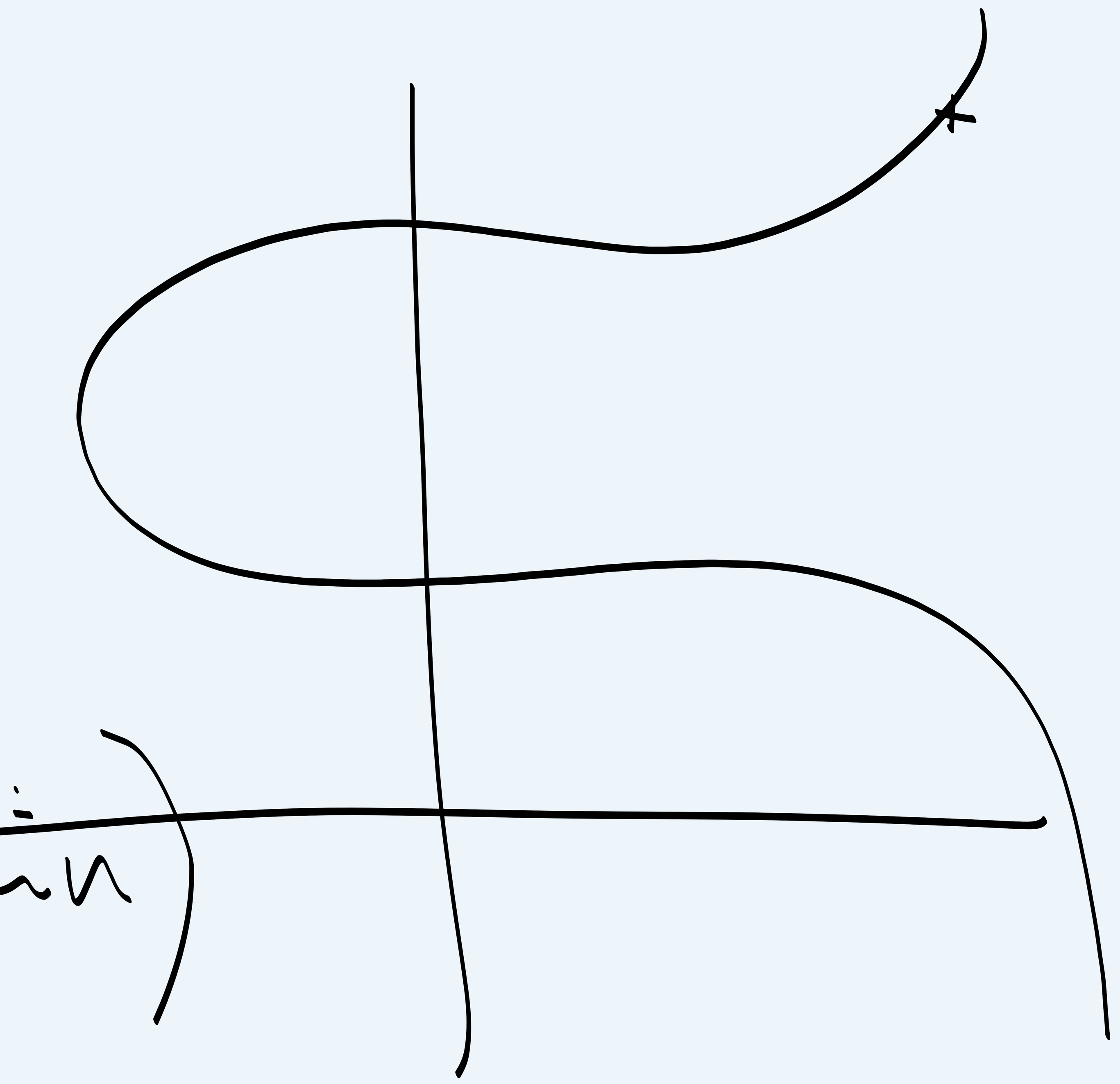
1) Based on factorization:

   Given $\underline{n} = p \cdot q$, $p, q$ prime

   Find $p$ and $q$

2) Discrete log problems

3) Elliptic curve crypto (Blockchain)



$A \to E(m, PU_B) = C \to$ Secure $\to C \to D(C, PR_B) \to B$

$m$ $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $M$

All Systems have 3 algorithms:

1) KeyGen
2) Encryption $E$
3) Decryption $D$

## Key Generation:

1. Find/Buy two large primes, $(p, q) \geq 2048$ bits
2. $n = p \cdot q$
3. $\phi(n) = (p-1) \cdot (q-1)$
4. Choose Public Key $e$ s.t. $\gcd(e, \phi(n)) = 1$ Reg.
5. Calculate Private Key $d$ s.t. $e \cdot d \equiv 1 \mod \phi(n)$
   (Find invers of $e \mod \phi(n)$)

$PU = (e, n)$ → $n$ is always public.
$PR = (d, n)$

$PU = e$
$PR = d$

Encryption:

$$m^e \bmod n = c$$

Decryption:

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

---

E: $10^7 \bmod 187 = 175$

D: $175^{23} \bmod 187 = 10$

$m = 10$, $p = 11$, $q = 17$

① $11, 17$

② $n = 182$

③ $\phi(n) = 10 \cdot 16 = 160$

④ $e = 7$ check: $\gcd(160, 7) \stackrel{?}{=} 1$

⑤ $e \cdot d \equiv 1 \bmod \phi(n)$

$d = 23$, $e = 7$