Date:

# Cryptography 101

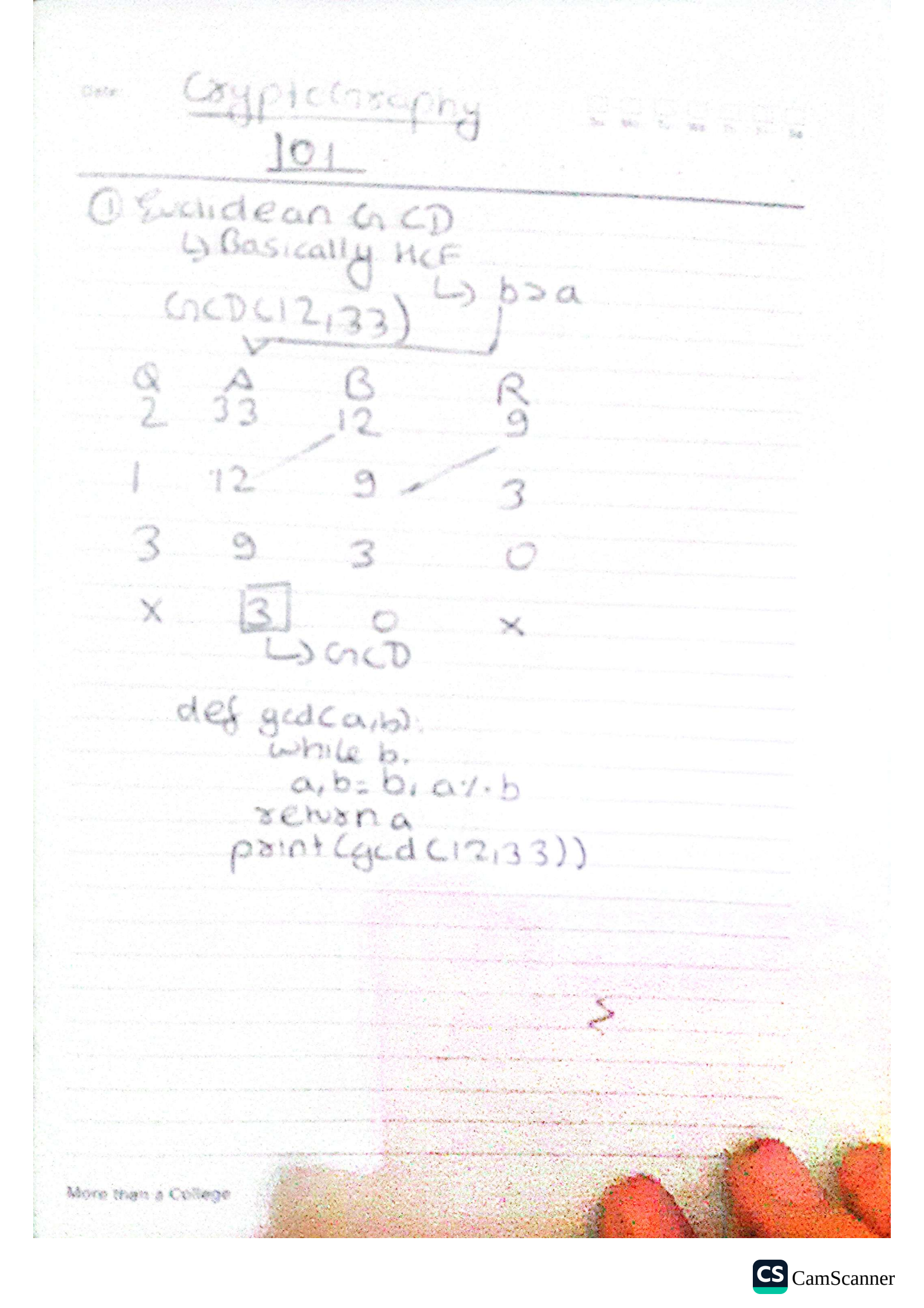
① Euclidean GCD
↳ Basically HCF
↳ b > a

GCD(12,33)

| Q | A | B | R |
|---|---|---|---|
| 2 | 33 | 12 | 9 |
| 1 | 12 | 9 | 3 |
| 3 | 9 | 3 | 0 |
| x | [3] | 0 | x |

↳ GCD

```
def gcd(a,b):
    while b:
        a,b = b, a%b
    return a
print(gcd(12,33))
```



## Multiplicative inverse

↳ Numbers when multiplied give 1

$5 \times 5^{-1} = 1$, $A \times A^{-1} = 1$

---

# Extended GCD (Multiplicative Inverse using EEA) → a > b

What's M.I of 3 mod 5?

| Q | A | B | R | $T_1$ | $T_2$ | T |
|---|---|---|---|---|---|---|
| 1 | 5 | 3 | 2 | 0 | 1 | -1 |
| 1 | 3 | 2 | 1 | 1 | -1 | 2 |
| 2 | 2 | 1 | 0 | -1 | 2 | -5 |
| X | 1 | 0 | X | 2 | -5 | X |

↳ M.I is 2

$T_1 = 0$ & $T_2 = 1$

$T = T_1 - T_2 \times Q$

```
def egcd(a,b):
    if b==0;
      return a,1,0
    gcd,x,y = egcd(b, a%b)
      u=y
      v=x-(a//b)*y
    return gcd,u,v.

p=26513
q=32321
gcd,u,v = egcd(p,q).
```

# a ≡ b (mod m)

↳ Div 'a' by 'm', such that remainder is b.

# fermat's Little theasem

↳ If 'p' is paime number & 'a' is the integer not divisible by p then

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

# Does FLT hold for p=5 & a=2

Sol

p=5 & a=2

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

$2^{6-1} = 1 \pmod{5}$

$16 \equiv 1 \pmod{5}$ True

# Multiplicative Inverse

$g \cdot d \equiv 1 \pmod{p}$

F·L·T gives shortcut,

$g^{p-1} \equiv 1 \pmod{p}$.

$g^{p-2} = g^{-1} \pmod{p}$

So inverse of g modulo p is

$$d = g^{p-2} \bmod p$$

# Quadratic Residues

$x^2 \equiv c \pmod{p}$

$x^2 \equiv 3 \pmod{5}$ = No solution
i.e no quadratic residue.

If there is solution we say c is quadratic residue (mod p).

3 is not quadratic residue $\pmod{5}$.

- Every quadratic residue has two roots modulo p: a & -a mod p.
- Half numbers 1, 2, ... p-1 are Q.R & half are not Q.R.

p = 29
ints = 14, 6, 11

find, which of these numbers is Q.R modulo 29. find its square root(s) & return smaller root.

- Every Q.R modulo has exactly 2 roots: a & p-a #

# Legendre Symbol

a) First Property of Quadratic Non-Residues:

| |
|---|
| QR * QR = QR |
| QR * QNR = QNR |
| QNR * QNR = QR |

b) Legendre Symbol is effecient way to determine whether integer is a ~~QR~~ Q.R.

Date:

Su Mo Tu We Th Fr Sa

For odd prime p, & int a:

$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is Q·R mod } p \\ -1 & \text{if } a \text{ is QNR mod } p \end{cases}$

↳ Legendre Symbol (L·S)

# Modular square Root

↳ L·S introduced fast way to find if number is a square root modulo 'a' prime 'p'.

↳ More efficient way is ↓

# Tonelli-Shanks Algo

↳ All prime that ain't 2 are of form $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$,

↳ Simple formula:

$$root = a^{(p+1)/4} \bmod p$$

↳ Mainly used in finding Elliptic curve coordinates

Coprime = Pairs of ints whose HCF is 1 only.

Date: Su Mo Tu We Th Fr Sa

---

# Chinese Remainder Theorem (CRT)

4) Gives unique solution to set of linear congruences if their moduli are coprime.

$$\left.\begin{aligned} x &= a_1 \pmod{m_1} \\ x &= a_2 \pmod{m_2} \\ &\dots \\ x &= a_n \pmod{m_n} \end{aligned}\right\} \text{congruence}$$

(5 steps, 2 weights)

CRT states that above equations have unique solution of moduli that are relatively prime.

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \dots + a_n M_n M_n^{-1}) \bmod M$$

# Solve eqn using CRT

$$x = 2 \pmod 3$$
$$x = 3 \pmod 5$$
$$x = 2 \pmod 7$$

So

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

Date:

| Given, | | To find | | |
|---|---|---|---|---|
| $a_1 = 2$ | $m_1 = 3$ | $M_1$ | $M_1^{-1}$ | M |
| $a_2 = 3$ | $m_2 = 5$ | $M_2$ | $M_2^{-1}$ | |
| $a_3 = 2$ | $m_3 = 7$ | $M_3$ | $M_3^{-1}$ | |

$$M = m_1 \times m_2 \times m_3$$
$$= 3 \times 6 \times 7 = 105$$

$$M_1 = \frac{M}{m_1} = 35$$

$$M_2 = \frac{M}{m_2} = 21$$

$$M_3 = \frac{M}{m_3} = 15$$

X we know,

$$M_1 \times M_1^{-1} = 1 \bmod m_1$$
$$35 \times M_1^{-1} = 1 \bmod 3$$

$$M_1^{-1} = 2 \#$$

Similarly,

$$M_2^{-1} = 1$$

$$M_3^{-1} = 1$$

$X = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$

$= 233 \bmod 105$

$\therefore X = 23$ #

# Modular Binomials

Reassuring following eqn to get p, q Primes

$N = p \cdot q$

$c_1 = (2p + 3 \cdot q)^{e_1} \bmod N$

$c_2 = (5 \cdot p + 7 \cdot q)^{e_2} \bmod N$

$N = \ldots$

$e_1 = \ldots$

$e_2 = \ldots$

$c_1 = \ldots$

$c_2 = \ldots$

Soln

$c_1^{e_2} = (2p + 3q)^{e_1 e_2} \bmod N$

Multiply $c_1^{e_2}$ by Square

N is product of 2 primes

$c_1$ & $c_2$ are modular exponentiations of linear combination of p & q

$$c_1^{e_2} = (2p+3q)^{e_1 e_2} \pmod N$$

$$c_2^{e_1} = (5p+7q)^{e_1 e_2} \pmod N$$

Aligns both ciphers to same exponent $e_1 e_2$ Now,

Multiply by constant to align linear coefficient

Multiply $c_1^{e_2}$ by $5^{e_1 e_2}$

$$\delta_1 = 5^{e_1 e_2} \cdot c_1^{e_2}$$
$$= (5 \cdot (2p+3q))^{e_1 e_2}$$
$$= (10p+15q)^{e_1 e_2} \pmod N$$

Multiply $c_2^{e_1}$ by $2^{e_1 e_2}$

$$\delta_2 = 2^{e_1 e_2} \cdot c_2^{e_1}$$
$$= (2 \cdot (5p+7q))^{e_1 e_2}$$
$$\equiv (10p+14q)^{e_1 e_2} \pmod N$$

Now, p coeff are 10.
q coeff differs by 1.

Subtract & isolate q

$$\delta_1 - \delta_2 \equiv (10p + 16q)^{e_1 e_2} - (10p + 11q)^{e_1 e_2} \pmod{N}.$$

or, $\delta_1 - \delta_2 = q^{e_1 e_2} \pmod{N}.$

or, $q = gcd(\delta_1 - \delta_2, N)$

Now, once q is known,

$\therefore p = N // q$ #