## CS 304 (Theory)

Ph - 9474957559.6

Pre Midterm → 10 marks

Midterm → 10 marks + 10 marks

Pre Endterm → 15 marks

Endterm → 15 marks + 15 marks

Rem 25 marks = Attendance + Assignments + Class test

## CS 364

All the coding will be in C

Assignments → 3 or 4 (80 to 90 marks)

Continuous Assesment → 10 or 20 marks

- Cryptography → The part where we develop algorithms to get Security / Designing the Algo
- Cryptanalysis → We try to break the Security of designed algorithm

Cryptology = Cryptography + Cryptanalysis

NIST → Standardizes Cryptographic Algos.

ATM 1 → PIN 1 + X = $Y_1$ → write

ATM 2 → PIN 2 + X = $Y_2$ → write

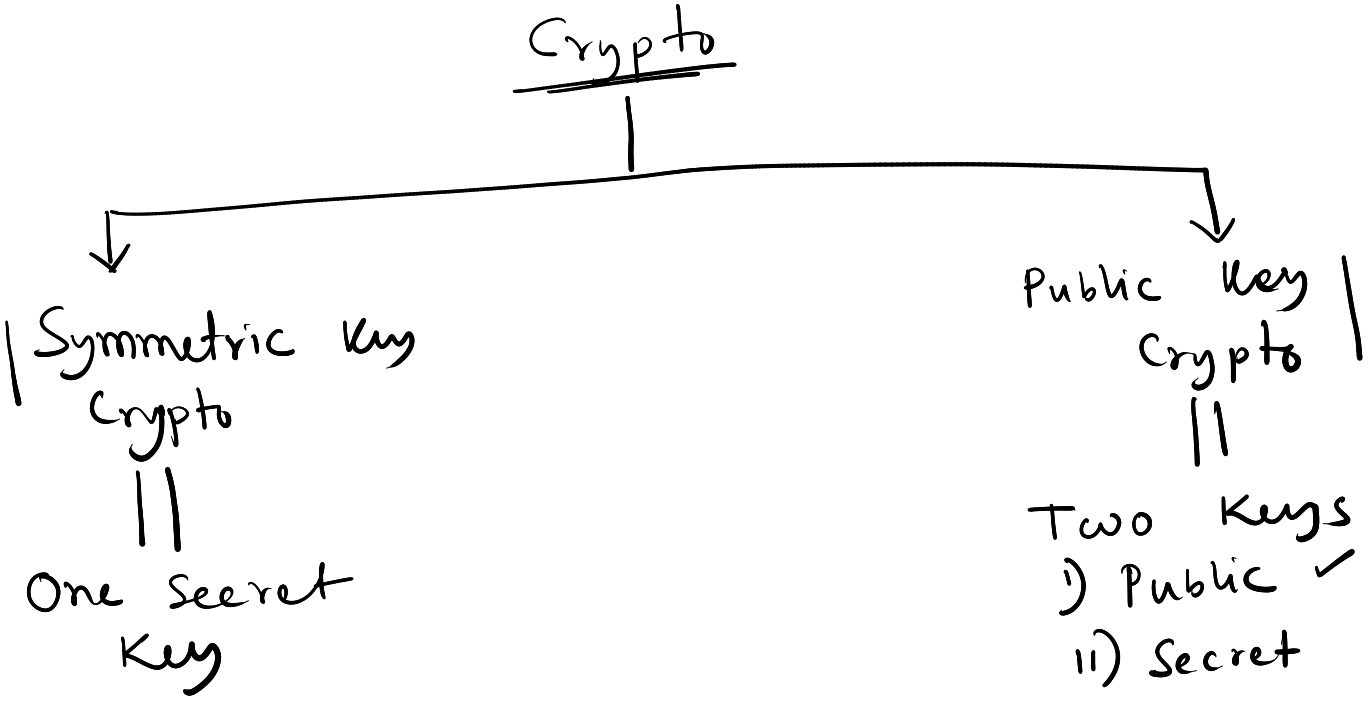
ATM 3 → PIN 3 + X = $Y_3$ → write

ATM 10 → PIN 10 + X = $Y_{10}$ → write

X → Secret

↓

Secret Key


Crypto
Symmetric Key Crypto
One Secret Key
Public Key Crypto
Two Keys
i) Public
ii) Secret

Cryptography provides following Security Services :-

i) Confidentiality ✓

ii) Integrity ✓

iii) Authentication ✓

iv) Non-repudiation

## i) Confidentiality (secrecy)

Ensuring that no one can read the message except the intended receiver

The original data can't be recovered without the proper credential even if the data is transferred via an insecure channel.

## ii) Integrity (anti-tampering)

Assuring the receiver that the received message has not been altered in any way from the original.

## iii) Authentication

verification of one's identity.

iv) Non repudiation

A mechanism to prove that the Sender really sent this message.

---

## Confidentiality

i) Plaintext :→ original message

ii) Encryption Algorithm → function

iii) Ciphertext → un-readable form of plaintext

iv) Decryption Algorithm → function

v) Encryption Key → Key

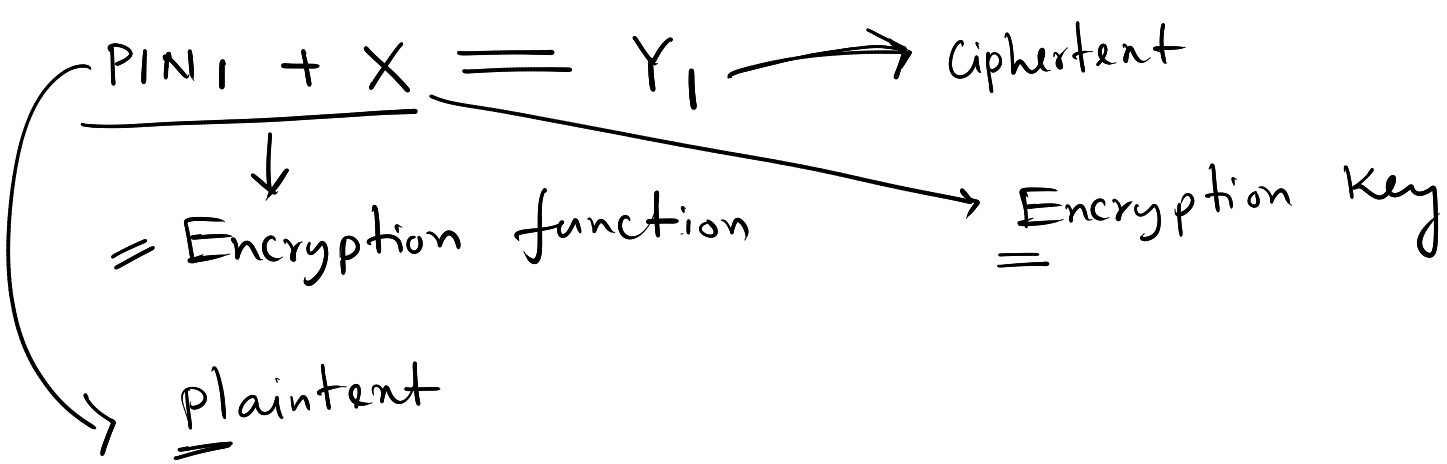
vi) Decryption Key → Key

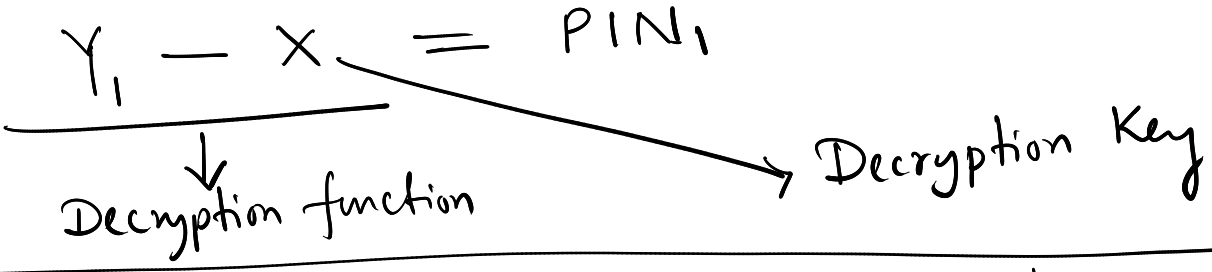
✓ Encryption function $\left(\underset{\text{plaintext}}{\vec{M}}, \text{Enc.Key}\right)$ = Ciphertext

Enc. func : $P \times \text{Enc.Key} \longrightarrow \underset{(C)}{\text{Ciphertext}}$

✓ Decryption function (Ciphertext, Dec. Key) = plaintext = M

Dec. func : $C \times \text{Dec.Key} \longrightarrow P$




Cryptography

- E → Encryption
- D → Decryption

Symmetric key

$E(M, K) = C$

$D(C, K) = M$

Public key / Asymmetric key

$E(M, PK) = C$

$D(C, SK) = M$

$PK \neq SK$

## CAESAR Cipher

This cipher is named after Julius Caesar

It relies on shifting the letters of a message by an agreed number

agreed number = 3

Encryption ↓

plaintext → INTERNET

agreed number = 3 → Secret key

Ciphertext → LQWHUQHW=

Decryption ↓

INTERNET

## Function

$f: A \longrightarrow B$ it is a relation between the elements of A and B with the property that if $a, b \in A$ and $a = b$ then $f(a) = f(b)$

## one to one function

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

## onto function

$f: A \rightarrow B$

then $\forall\, b \in B \;\; \exists \;\; a \in A$ s.t. $f(a) = b$

## Bijective function

$f: A \rightarrow B$ is bijective function iff $f$ is one to one and onto

## Permutation

Let $\pi$ be a permutation on a set S

then $\pi: S \longrightarrow S$ is a bijection from S to S

$$\pi: \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

## One way Function

$f : X \longrightarrow Y$ is called a one way if given $x \in X$ it is easy to compute $f(x)$ but given $f(x)$ it is hard to find $x$.

Ex. $p$ is a prime (large), $q$ is a prime (large) → Given

$N = p \times q$ → this computation is easy

Given $N$ find $p, q$ s.t. $N = p \times q$

($p, q$ ↓ large primes)

is hard

## Substitution Box

$S : A \longrightarrow B$ with $|B| \leq |A|$

$S : \{1,2,3,4\} \longrightarrow \{1,2,3\}$

$S(1) = 1 \quad S(2) = 3 \quad S(3) = 2$

$S(4) = 1$

## Transposition Cipher

$M = m_1 m_2 \cdots m_t \rightarrow$ plaintext

$e$ : permutation on $t$ elements $\rightarrow$ Secret Key

$\{1, 2, \cdots t\}$

**Encryption**

$$c = m_{e(1)} m_{e(2)} \cdots m_{e(t)} = c_1 c_2 \cdots c_t$$

$\hookrightarrow$ Ciphertext

**Decryption**

$$M = c_{e^{-1}(1)} \cdots c_{e^{-1}(t)}$$

ex. Plaintext : CAESAR $= m_1 m_2 \cdots m_6$

Secret key $e$ :

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| 6 | 4 | 1 | 3 | 5 | 2 |

Encryption

Ciphertext : RSCEAA $= c_1 c_2 c_3 \cdots c_6$

$d = e^{-1}$ :

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| 3 | 6 | 4 | 2 | 5 | 1 |

Decryption

plaintext : CAESAR

## Substitution Cipher

$M = m_1 m_2 \cdots m_L$

$\mathcal{A} = \{A, B, C, \cdots Z\}$, $m_i \in \mathcal{A}$

$e$ : Substitution from $\mathcal{A}$ to $\mathcal{A}$

$e \rightarrow$ Secret key

Encryption $C = e(m_1)\, e(m_2)\, e(m_3) \cdots e(m_L)$

ex: $e(A) = Z$, $e(B) = D$, $\cdots e(C) = A$

ABC → plaintext

ZDA → ciphertext

---

## Affine Cipher

| A | B | C | ⋯ | Z |
|---|---|---|---|---|
| ↓ | ↓ | ↓ | | ↓ |
| 0 | 1 | 2 | | 25 |

$\mathcal{A}$ → set of alphabates

$\mathcal{A} \longrightarrow \mathbb{Z}_{26}$

$K$ = Secret key $= (a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$

Encryption function

$e(x, K) = (a \cdot x + b) \bmod 26$

$= C$

## Decryption function

$$d(c, K) = \left((c - b) \cdot a^{-1}\right) \bmod 26$$

## Affine cipher

$Z_{26} = \{0, 1, \ldots 25\}$

$Z_{26}^* = Z_{26} \setminus \{0\}$

Secret key $K = (a, b) \in Z_{26}^* \times Z_{26}$

plaintext $x \in Z_{26}$

$\boxed{\gcd(a, 26) = 1}$

Enc : $c = E(x, K) = (a \cdot x + b) \bmod 26$

Dec : $x = D(c, K) = (c - b) \cdot a^{-1} \bmod 26$

---

## $Z_6 = \{0, 1, 2, 3, 4, 5\}$

$+ \bmod 6 : +_6$

$x, y \in Z_6$

$z = (x + y) \% 6$

0 : additive identity

| $+_6$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

$(x + y) \% 6 = 0$

Every element of $Z_6$ with $+_6$ has an additive inverse

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ multiplication modulo 6

$*_6$

$x, y \in \mathbb{Z}_6 \quad x * y = z \;\%\; 6 = y = x *_6 y$

| $*_6$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | **1** |

1: is the multiplicative identity

$(x * y) \;\%\; 6 = 1$

1, ~~2~~, ~~3~~, ~~4~~, 5

$0 \neq x \in \mathbb{Z}_6$ ~~iff~~ $\gcd(x, 6) = 1$ then $\exists\, y$ s.t $x *_6 y = 1$

$0 \neq x \in \mathbb{Z}_m \quad \cdot \gcd(x, m) = 1$

$\Leftrightarrow \quad x *_m y = 1$

$x * y \equiv 1 \pmod m$

$\Rightarrow \quad m \mid (xy - 1)$

$\Rightarrow \quad xy - 1 = t \cdot m$

$\Rightarrow \quad 1 = t_1 m + xy$

$\Rightarrow \quad \gcd(x, m) = t_1 m + xy$

To find $(t_1, y)$ we have follow Extended Euclidean Algorithm

---

☑ $\mathbb{Z}_m^*$ $\quad a \in \mathbb{Z}_m^*$ $\quad *_m$

Read

a will be invertible iff $\gcd(a, m) = 1$

$\phi(m)$ : Euler phi function

↳ # $x$, $0 < x \leq m-1$ s.t. $\gcd(x, m) = 1$

---

☑ Playfair Cipher $\quad I = J$

Secret key = Playfair example

| | | | | |
|---|---|---|---|---|
| P | L | A | Y | F |
| I | R | E | X | M |
| B | C | D | G | H |
| K | N | O | Q | S |
| T | U | V | W | Z |

Plaintext : HIDE

HI → BM

DE → OD

Ciphertext : BMOD

SACHIN

CSEX

MSG → CSE → CSEx (odd length)

MSG → BALL

BA LX LX

Add extra X to make the msg of even length

Add extra X in between two repeated letter

i) If both letters are the same (or only one letter is left) add an 'X' after the first (last) letter. Encrypt the new pair and continue.

ii) If the letters appear on the same row of your table, replace them with the letter to their immediate right respectively

iii) If the letters appear on the same column of your table, then replace them with the letters immediately below respectively

iv) If the letters are not in the same row or column, then replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important — the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair

## Hill Cipher

$A = (a_{ij})_{n \times n}$ → invertible matrix

↳ Secret Key

$M = (m_1 m_2 \cdots m_n)$ → Plaintext

**Encryption**

$C = A \cdot M = (c_1 \cdots c_n)$

**Decryption**

$M = A^{-1} \cdot C$

---

$S : \{A, \cdots, Z\} \rightarrow \{A, \cdots, Z\}$

$P \rightarrow C = S(P)$ $C \rightarrow$ Known

↳ Secret Key

$\# S = 26! \approx 2^{122}$

Brute force attack / Exhaustive Search

## Kerchoff's Rule

Design has to be public

## Shanon's notion of perfect secrecy

E → Encryption algo

M → Message

C → Ciphertext

$E(M) = C$ ↓ going via public channel

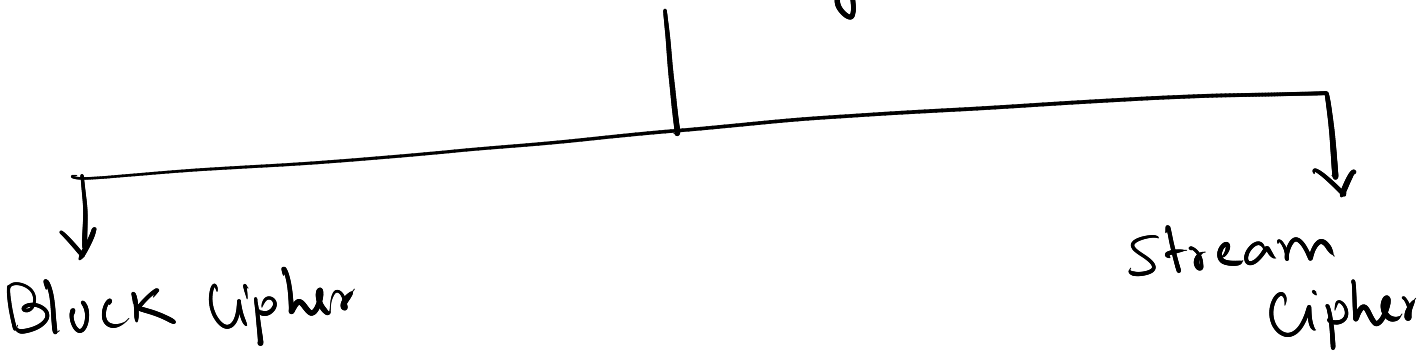
E will be providing perfect secrecy iff the ciphertext does not reveal any information regarding the plaintext/message

$$Pr[M = m \mid C = c] = Pr[M = m]$$

$$Pr[\text{message} \mid \text{ciphertext}] = Pr[\text{message}]$$

OTP

# Symmetric key Cipher




## Block Cipher

$$M = m_0 \| m_1 \| m_2 \| \cdots \| m_n$$

Block

length of $m_i = l$

Enc → it can encrypt $l$ length message

We can do the encryption on M using Enc blockwise

In block cipher encryption is done Blockwise

Ex. $M = m_0 \| m_1 \| \cdots \| m_l$

Encryption $C = Enc(m_0, K) \| Enc(m_1, K) \| \cdots \| Enc(m_l, K)$

$C = c_0 \| c_1 \| \cdots \| c_l$

Decryption

$$M = Dec(C_0, K) \| Dec(C_1, K) \| \ldots \| Dec(C_l, K)$$

## Stream cipher

$$M = m_0 \cdots m_l$$

where $m_0 \in \{0, 1\}$

Encryption → It will be performed bitwise

$$C = \underset{C_0}{(m_0 \oplus z_0}, \underset{C_1}{m_1 \oplus z_1}, \cdots, \underset{C_l}{m_l \oplus z_l})$$

Dec ↑ $M = C_0 \oplus z_0, C_1 \oplus z_1 \cdots C_l \oplus z_l$

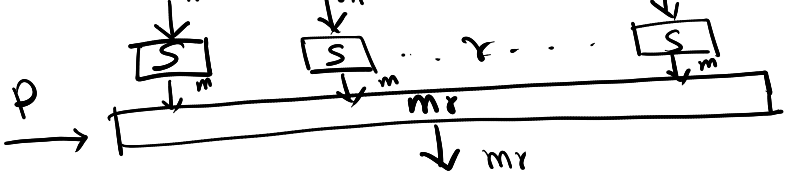
## Product cipher

A product cipher Combines two or more trasformations in a manner intending that the resulting cipher is more secure than the individual transformation.

## Substitution Permutation Network (SPN)

It is a product cipher based Substitution box and permutation box.

ex. $S: \{0,1\}^n \longrightarrow \{0,1\}^m$, $P: \{0, \ldots mr-1\} \longrightarrow \{0, \ldots mr-1\}$




len (input) = nr

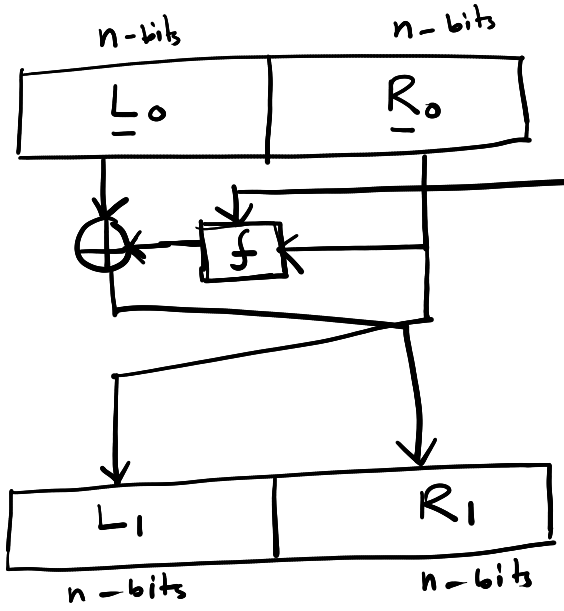
# Feistel Network (FN)

# Feistel Network (FN)

- P → plaintext of size $2n$-bits
  - $P = L_0 \| R_0$ ($n$ bits, $n$ bits)

$K$ → Secret Key
$len(K) = l$-bits

Encryption
one round FN




$$f : \{0,1\}^n \times \{0,1\}^l \longrightarrow \{0,1\}^n$$

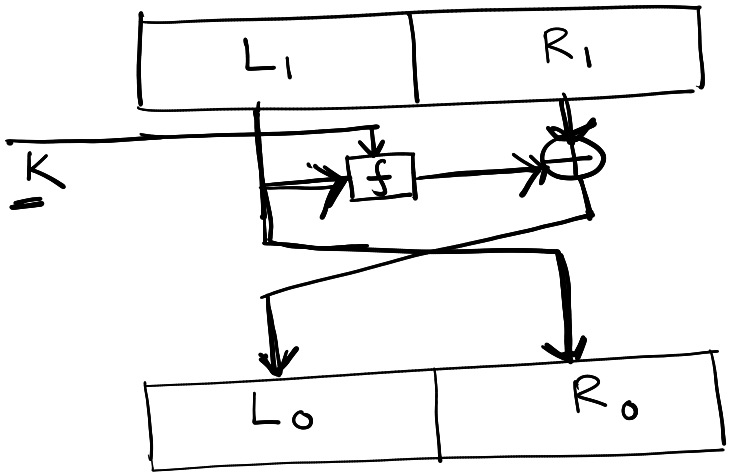
$$L_1 = R_0$$
$$R_1 = L_0 \oplus f(R_0, K)$$

- $C = L_1 \| R_1$ → Ciphertext

Decryption

$$f(L_1, K) = f(R_0, K)$$

- $R_0 = L_1$
- $L_0 = R_1 \oplus f(L_1, K)$




Inversion of $f$ is not required.

## I) Data Encryption Standard (DES)

→ is based on Feistel Network (FN)

## II) Advanced Encryption standard (AES)

→ is based on SPN

---

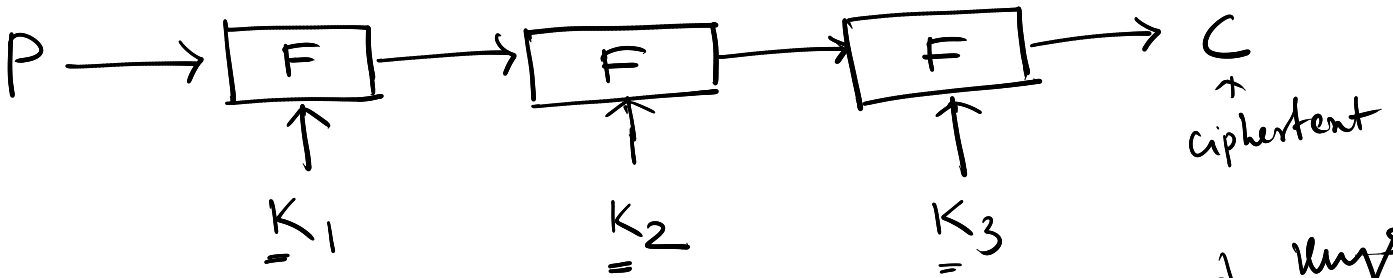
## Iterated block cipher

An Iterated block cipher is block cipher involving the Sequential repetition of an internal function (called as **Round function**). The parameters include the number of **rounds r**, the **block size n**, and the **round keys $K_i$** of length l generated from the original secret key K.

ex.

F → round function
P → plaintext block
K → secret key

3-round block cipher




$G(K) \rightarrow K_1, K_2, K_3$ → round keys

↳ Keyscheduling function (Algo)

# OTP (one time padding)

OTP provides perfect secrecy under some conditions.

**Encryption**

$P \rightarrow$ plaintext

$K \rightarrow$ Secret key

$\oplus$ bitwise xor

- $Enc(P, K) = P \oplus K = C$

**Decryption**

- $Dec(C, K) = C \oplus K = P$

- $Pr[\text{message} \mid \text{Ciphertext}] = Pr[\text{message}]$

**Conditions**

1) The Secret key K Cannot be used to encrypt two messages
2) length (K) $\geq$ length (P)
3) K is uniformly selected from the key space

# OTP on one bit enc

message $\leftarrow m \in \{0,1\}$, $k \xleftarrow{uniformly} \{0,1\}$

- $Pr[m=0] = p$
- $Pr[m=1] = (1-p)$
- $Pr[k=0] = \frac{1}{2}$
- $Pr[k=1] = \frac{1}{2}$

Encryption $\quad c = m \oplus k$

$$Pr[c=0] = Pr[m=0, k=0] + Pr[m=1, k=1]$$

$$= Pr[m=0] \cdot Pr[k=0] + Pr[m=1] \cdot Pr[k=1]$$

$$= \left(p \times \frac{1}{2}\right) + \left((1-p) \times \frac{1}{2}\right)$$

$$= \frac{1}{2}$$

Similarly

$$Pr[c=1] = \frac{1}{2}$$

$$Pr[M = m \mid C = c] \stackrel{?}{=} Pr[M = m]$$

i) $Pr(A|B) = \frac{Pr(AB)}{Pr(B)}$

ii) $Pr(AB) = Pr(B|A).P(A)$

$$Pr[M = 0 \mid C = 0]$$

$$= \frac{Pr[M = 0,\ C = 0]}{Pr[C = 0]}$$

$$= \frac{Pr[C = 0 \mid M = 0] \times Pr[M = 0]}{1/2}$$

$$= \frac{Pr[K = 0] \times Pr[M = 0]}{1/2}$$

$$= \frac{\frac{1}{2} \times Pr[M = 0]}{1/2}$$

$$= Pr[M = 0]$$

- $Pr[M = 0 \mid C = 0] = Pr[M = 0]$

Thus it provides perfect Secrecy

## Conditions

1) $M_1 \oplus K = C_1$
   $M_2 \oplus K = C_2$
   ] this will reveal information on messages.

$$C_1 \oplus C_2 = (M_1 \oplus K) \oplus (M_2 \oplus K)$$
$$= M_1 \oplus M_2$$

ciphertexts difference will give you message difference

11) $len(K) < len(P)$

$$C = P \oplus K$$

$P = P_1 \cdots P_l \quad P_n$

$\oplus$ $K = K_1 \cdots K_l K_i \cdots K_t$

$C = \underbrace{(P_1 \oplus K_1)}_{C_1} (P_2 \oplus K_2) \cdots (P_l \oplus K_l) \underbrace{(P_{l+1} \oplus K_1)}_{C_{l+1}} \cdots (P_n \oplus K_t)$

$C_1 \oplus C_{l+1} = P_1 \oplus P_{l+1}$

* $len(K) \geq len(P)$

* OTP is not usuable in real life

☑ OTP is not usuable in daily life

→ I) Secret key cannot be reusable. Only one message can be encrypted using the key

II) length (Key) ≥ length (message)

Due to (I), (II) OTP is not practical.

---

☑ Data Encryption Standard (DES)

- It is a block cipher
- Designed by IBM

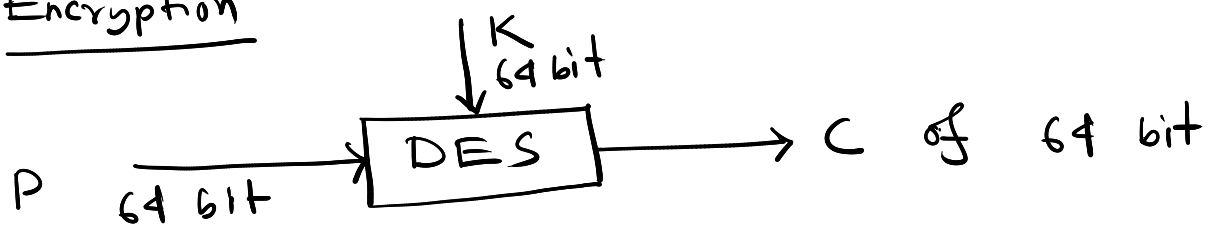
I) Block size = 64 bit

II) Number of rounds = 16

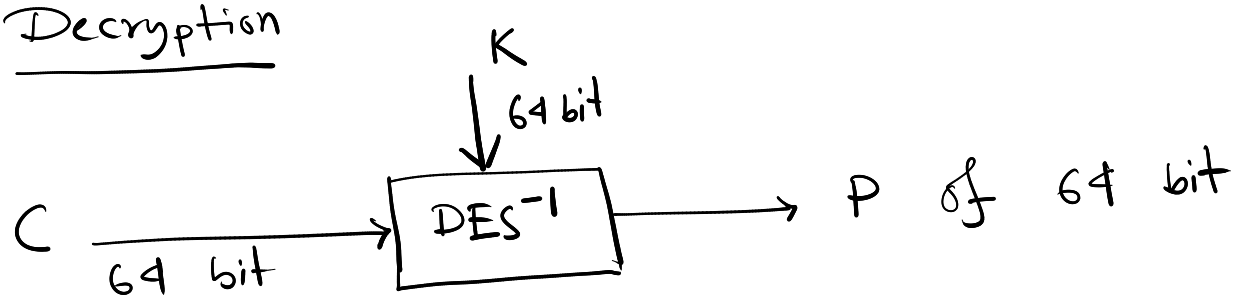
III) Secret key size = 64 bit with 8 parity check bits.

IV) It is based on Feistel Network

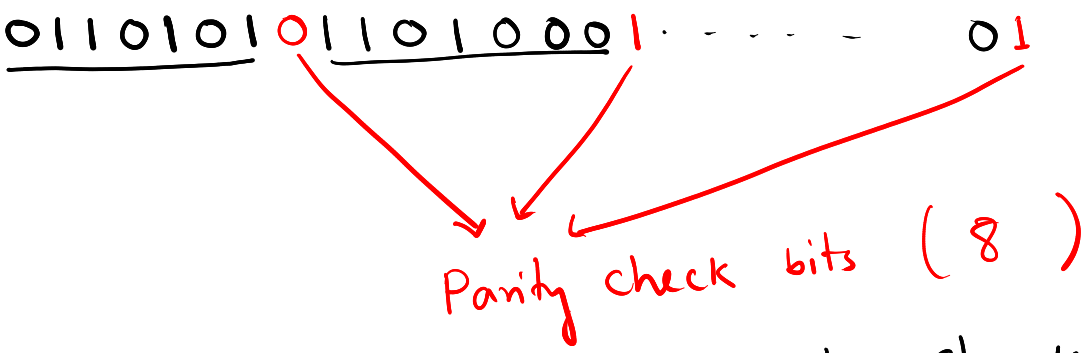
Encryption



## Decryption




☑ Secret Key is 64 bit with 8 parity check bits




After discarding 8 parity check bits
→ the final secret key will be of 56 bit

DES should provide 56 bit security

---

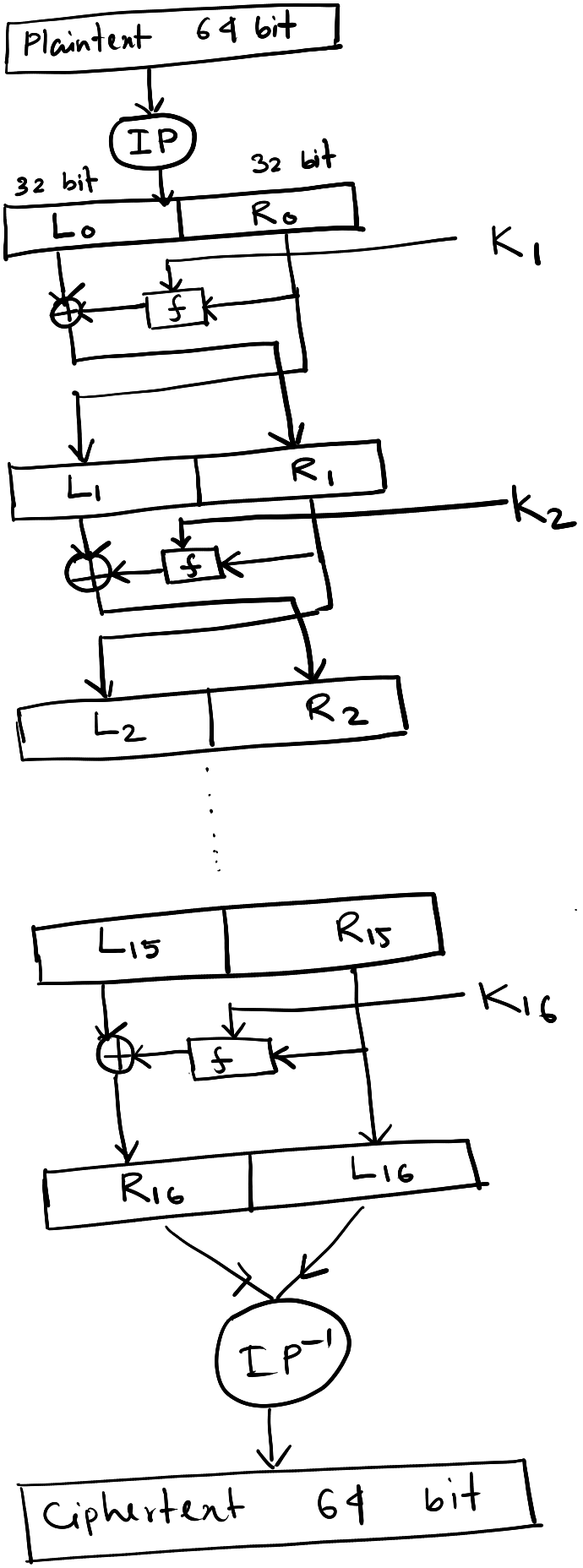
☑ In DES we have 16 round key $K_1, K_2, \ldots, K_{16}$ which are generated using key scheduling algorithm

Key scheduling algo will take the secret key as an input

length $(K_i) = 48$ bits

# Structure of DES

Encryption




$L_{i+1} = R_i \quad i = 0, \cdots 15$

$R_{i+1} = L_i \oplus f(R_i, K_{i+1})$

Think about Decryption

☑ We have to learn the followings

1) IP, $IP^{-1}$ ✓

2) what is f ? (round function)

3) How $K_1, \ldots K_{16}$ (round keys) are generated ?

## ☑ IP (Initial permutation)

$$IP : \{0,1\}^{64} \longrightarrow \{0,1\}^{64}$$

Handbook (PP – 253)

IP :

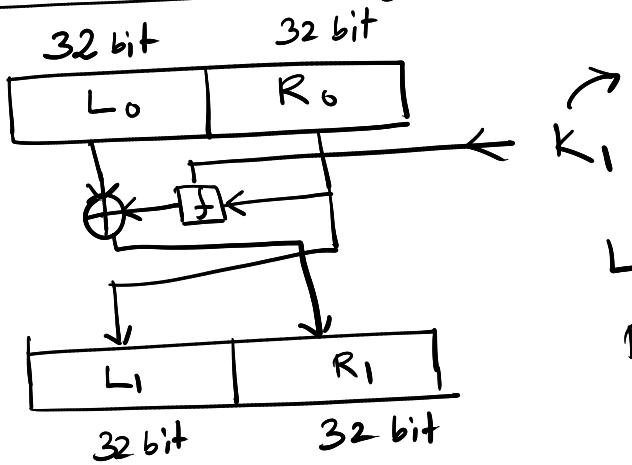
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| ⋮ | | | | | | | |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

$IP(m_1 m_2 \ldots m_{64})$

$= (m_{58}\ m_{50}\ m_{42}\ m_{34}\ m_{26} \ldots m_2\ m_{60}\ m_{52} \ldots m_4 \ldots m_{63}\ m_{55}\ m_{47} \ldots m_7)$

$IP^{-1}$

# Round function of DES




$L_1 = R_0$

$R_1 = L_0 \oplus f(R_0, K_1)$

- $f : \{0,1\}^{32} \times \{0,1\}^{48} \longrightarrow \{0,1\}^{32}$

$$f(R_i, K_i) = X_i$$

where $R_i$ is 32 bit

$K_i$ is 48 bit

$X_i$ is 32 bit

$$f(R_i, K_i) = P\left(S\left(E(R_i) \oplus K_i\right)\right)$$

- ✓ $E : \{0,1\}^{32} \longrightarrow \{0,1\}^{48}$ (Expansion function)
- ✓ $S : \{0,1\}^{48} \longrightarrow \{0,1\}^{32}$ (Substitution box)
- ✓ $P : \{0,1\}^{32} \longrightarrow \{0,1\}^{32}$ (Permutation box)

$E : \{0,1\}^{32} \longrightarrow \{0,1\}^{48}$

$E(x_1, x_2, \cdots x_{32}) = (y_1 \cdots y_{48})$

Handbook → PP 253

E :

| | | | | | |
|---|---|---|---|---|---|
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

$E(x_1, \cdots x_{32})$

$= (x_{32}\ x_1\ x_2\ x_3\ x_4\ x_5$
$x_4\ x_5\ x_6\ x_7\ x_8\ x_9$
$x_8\ x_9\ x_{10}\ x_{11}\ x_{12}\ x_{13}$
$x_{12}\ x_{13}\ x_{14}\ x_{15}\ x_{16}\ x_{17}$
$x_{16}\ x_{17}\ x_{18}\ x_{19}\ x_{20}\ x_{21}$
$x_{20}\ x_{21}\ x_{22}\ x_{23}\ x_{24}\ x_{25}$
$x_{24}\ x_{25}\ x_{26}\ x_{27}\ x_{28}\ x_{29}$
$x_{28}\ x_{29}\ x_{30}\ x_{31}\ x_{32}\ x_1)$

---

$S : \{0,1\}^{48} \longrightarrow \{0,1\}^{32}$

$S(X) = Y$ where X is 48 bit
Y is 32 bit

- $X = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8$
  where length of $B_i$ is 6-bit
- $S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8$

$S_i : \{0,1\}^6 \longrightarrow \{0,1\}^4 \quad \forall\ i = 1, 2, \cdots, 8$

$S_i(B_i) = C_i$

$B_i$: ↓ 6 bit, $C_i$: ↓ 4 bit

$$S(X) = \Big( S_1(B_1),\ S_2(B_2),\ S_3(B_3),\ S_4(B_4),\ S_5(B_5),\ S_6(B_6),\ S_7(B_7),\ S_8(B_8) \Big)$$

**$S(X) \rightarrow 32$ bit**

$$S_i : \{0,1\}^6 \longrightarrow \{0,1\}^4$$

Handbook → PP 253

$$S_i(B_i) = C_i$$

- $B_i = b_1 b_2 b_3 b_4 b_5 b_6$ $\quad b_i \in \{0,1\}$
- $r = (2 \times b_1 + b_6)$ $\quad 0 \le r \le 3$

  r is the integer representation of $(b_1 b_6)$
- $c$ = Integer representation of $(b_2 b_3 b_4 b_5)$ $\quad 0 \le c \le 15$

$S_i$ :

| r \ c | 0 | 1 | 2 | 3 | ... | 12 | ... | 15 |
|---|---|---|---|---|---|---|---|---|
| 0 | $a_{0,0}$ | $a_{0,1}$ | $a_{0,2}$ | | | | | $a_{0,15}$ |
| 1 | | | | | | | | |
| 2 | | | | | | → output | | |
| 3 | $a_{3,0}$ | $a_{3,1}$ | $a_{3,2}$ | | | | | $a_{3,15}$ |

$0 \le a_{i,j} \le 15$ $\quad$ 4 × 16

r → row number

c → column number

$S_i(B_i) = a_{r,c} \rightarrow 4$ bit

Handbook → PP 260

## Permutation P

$$P : \{0,1\}^{32} \longrightarrow \{0,1\}^{32}$$

P:

| | | | |
|---|---|---|---|
| 16 | 7 | 20 | 21 |
| 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 |
| 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 |
| 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 |
| 22 | 11 | 4 | 25 |

$$P(x_1, x_2, \ldots x_{32}) = (x_{16}, x_7, x_{20}, x_{21}, x_{29}, x_{12}, x_{28}, x_{17}, x_1, x_{15}, x_{23}, x_{26}, x_5, x_{18}, x_{31}, x_{10}, x_2, x_8, x_{24}, x_{14}, x_{32}, x_{27}, x_3, x_9, x_{19}, x_{13}, x_{30}, x_6, x_{22}, x_{11}, x_4, x_{25})$$

We have to understand Key Scheduling algorithm of DES

## DES

I) 16 rounds

II) 64 – bit block size

III) Key size = 64 bit

IV) IP and $IP^{-1}$

V) Round function

VI) Key scheduling Algo

---

## Key Scheduling Algo of DES

Input: 64 bit key K

Output: 16 round key $K_i$, $1 \le i \le 16$
where length of $K_i$ is 48 bit

I) Define $v_i$, $1 \le i \le 16$, where $v_i = 1$ if $i \in \{1, 2, 9, 16\}$ else $v_i = 2$

II) Discard 8 parity check bit from K.
The 56 bit key is $\tilde{K}$.

III) $T = PC1(\tilde{K})$; $PC1 : \{0,1\}^{56} \rightarrow \{0,1\}^{56}$

IV) $(C_0, D_0) = T$ where $C_0$ is of 28 bit
$D_0$ is of 28 bit

V) for $i = 1$ to 16

$$C_i = (C_{i-1} \hookleftarrow v_i)$$
$$D_i = (D_{i-1} \hookleftarrow v_i)$$

$\hookleftarrow$ left circular shift

$(x_1, x_2, \cdots x_{28}) \hookleftarrow 2 = (x_3, x_4, \cdots x_{28}, x_1, x_2)$

$$K_i = PC2(C_i, D_i)$$

$$PC2 : \{0,1\}^{56} \longrightarrow \{0,1\}^{48}$$

vi) Round keys $= (K_1, K_2, \cdots, K_{16})$

---

$PC1 : \{0,1\}^{56} \longrightarrow \{0,1\}^{56}$ | Handbook → PP 256

PC1 :

| $C_i$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 57 | 49 | 41 | 33 | 25 | 17 | 9 |
| | 1 | 58 | 50 | 42 | 34 | 26 | 18 |
| | 10 | 2 | 59 | 51 | 43 | 35 | 27 |
| | 19 | 11 | 3 | 60 | 52 | 49 | 36 |

| $D_i$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 63 | 55 | 47 | 39 | 31 | 23 | 15 |
| | 7 | 62 | 54 | 46 | 38 | 30 | 22 |
| | 14 | 6 | 61 | 53 | 45 | 37 | 29 |
| | 21 | 13 | 5 | 28 | 20 | 12 | 4 |

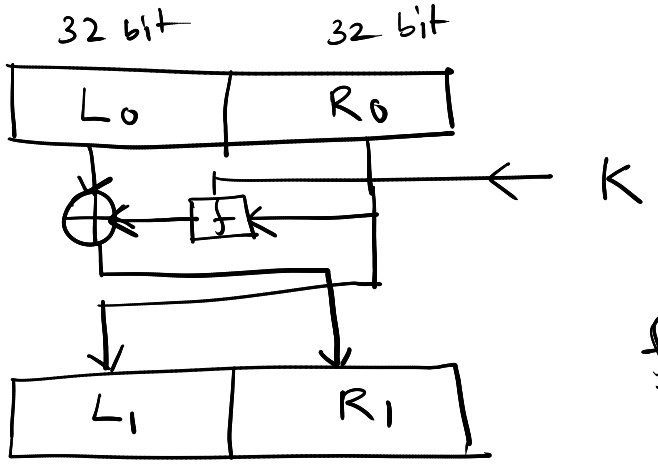
$PC1(K_1\ K_2 \cdots K_7\ K_9 \cdots K_{63})$

$= (K_{57}\ K_{49}\ K_{41}\ K_{33} \cdots K_9\ K_1\ K_{58} \cdots K_{36}$
$K_{63}\ K_{55} \cdots K_4)$

---

PC2 :

| | | | | |
|---|---|---|---|---|
| 14 | 17 | ⋯ | 5 | |
| 3 | 28 | ⋯ | 10 | |
| ⋮ | | | | 8 × 6 |
| 46 | 42 | — | 32 | |




$K \rightarrow 48$ bit

$$FN$$

$$f = P\left(S\left(E(R_0) \oplus K\right)\right)$$

$$M = L_0 \,\|\, R_0$$

$$C_1 = L_1 \,\|\, R_1$$

$$FN(M, K) = C_1$$

$$FN(\overline{M}, \overline{K}) = C_2$$

$\overline{X}$ : bitwise complement of $x$

$x = (x_1, \cdots x_{32})$

$\overline{x} = (1 \oplus x_1, \cdots, 1 \oplus x_{32})$

What will be the relation between $C_1$ and $C_2$ ?

$$L_1 = R_0$$

$$R_1 = L_0 \oplus f(R_0, K)$$

$$\overline{K} \oplus E(\overline{R_0}) = \overline{E(R_0) \oplus K}$$

$$= E(R_0) \oplus K$$

$$P\left(S\left(\overline{K} \oplus E(\overline{R_0})\right)\right) = P\left(S\left(E(R_0) \oplus K\right)\right)$$

$M, \quad K$

$L_0 \| R_0 = M$

$L_1 = R_0$

$R_1 = L_0 \oplus f(R_0, K)$

$f(R_0, K) = f(\bar{R}_0, \bar{K})$

$\bar{M}, \quad \bar{K}$

$\bar{L}_0 \| \bar{R}_0 = \bar{M}$

$\tilde{L}_1 = \bar{R}_0 = \bar{L}_1$

$\tilde{R}_1 = \bar{L}_0 \oplus f(\bar{R}_0, \bar{K})$

$= \bar{L}_0 \oplus f(R_0, K)$

$= \left(L_0 \oplus f(R_0, K)\right)$

$= \bar{R}_1$

$\tilde{L}_1 \| \tilde{R}_1 = \bar{L}_1 \| \bar{R}_1$

$C_2 = \bar{C}_1$

$(b_1 b_2 \cdots b_{56})$

$PC2(b_1 b_2 \cdots b_{56})$

$= (b_{14} b_{17} b_{11} b_{24} b_1 b_5 b_3 b_{28} \cdots b_{10} b_{23} \cdots b_8$
$b_{16} \cdots b_2 b_{41} \cdots b_{55} b_{30} \cdots b_{48} b_{44} \cdots b_{53}$
$b_{46} \cdots b_{32}) \rightarrow 48$ bits

---

## Attack models

### 1) Ciphertext only Attack

Attacker knows only ciphertexts

goal :- Recover the plaintexts corresponding to the ciphertexts or recover the secret key

### 2) Known plaintext Attack

Attacker knows some plaintexts and corresponding ciphertexts.

goal :- generate new plaintext, ciphertext pair or recover the secret key

### 3) Chosen plaintext Attack

Attacker chooses plaintexts according to his/her choice and (s)he will be provided the corresponding ciphertexts.

goal :- generate new plaintext, ciphertext pair or recover the secret key

## 4) Chosen Ciphertext Attack

Attacker chooses some ciphertext and he/she is allowed to get the corresponding plaintexts

goal:- Generate a new plaintext and ciphertext pair or recover the secret key

---

$$DES(M, K) = C$$

$$DES(\overline{M}, \overline{K}) = \overline{C}$$

Key = 56 bit
Brute force attack /Exhaustive search
$= 2^{56}$

$\Rightarrow$ Attacker chooses two plaintexts

i) $M$ ii) $\overline{M}$

Challenge is to find the key $K$

$$C_1 = DES(M, K)$$

$$C_2 = DES(\overline{M}, K)$$

CPA
choosen plaintext attack

Attacker is getting $C_1$ and $C_2$

$$DES(\overline{M}, \overline{K}) = \overline{C_2}$$

$$\Rightarrow DES(M, \overline{K}) = \overline{C_2}$$

$$Keys = \{ K_1, K_2, \cdots, K_{2^{56}} \}$$

Attacker selects $K_1 \in Keys$

He knows that $\overline{K_1} \in Keys$

Attacker performs $DES(M, K_1) = \tilde{C}$

if $\tilde{C} \neq C_1$ or $\tilde{C} \neq \overline{C_2}$

then discard $K_1, \overline{K_1}$ (why?)

if $\tilde{C} \neq C_1 \Rightarrow K_1 \neq K$

if $\tilde{C} \neq \overline{C_2} \Rightarrow K_1 \neq \overline{K} \Rightarrow \overline{K_1} \neq K$

In every search the attacker is able to discard two keys from the list

$$\frac{2^{56}}{2} = 2^{55} \rightarrow \text{Complexity for finding the key } K.$$

- DES → is not secure due to multiple attacks

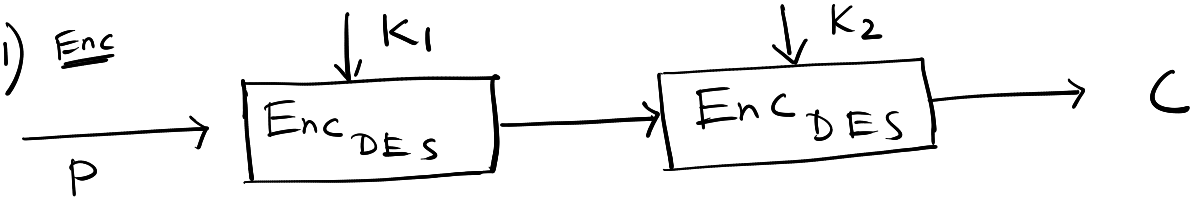
- Increase the length of the Secret Key

- Double Encryption

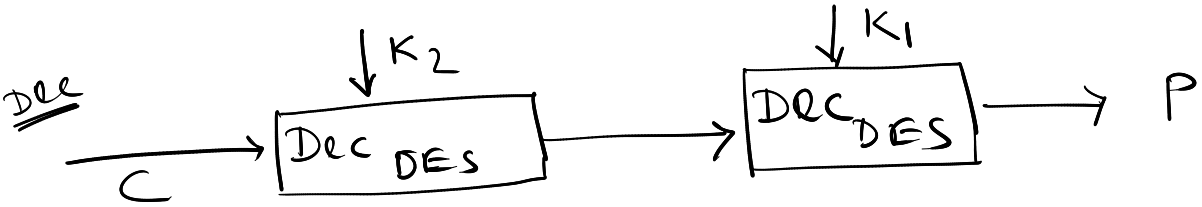
$$K = K_1 \| K_2$$

length of $K_1$ = 56 bit
" " $K_2$ = 56 bit
$\Rightarrow$ len(K) = 112 bit

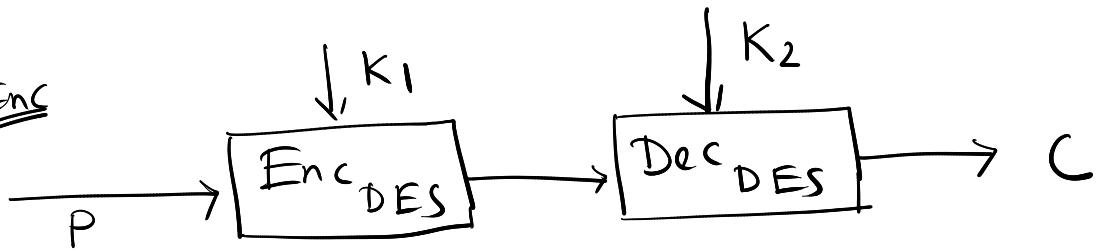
1) Enc



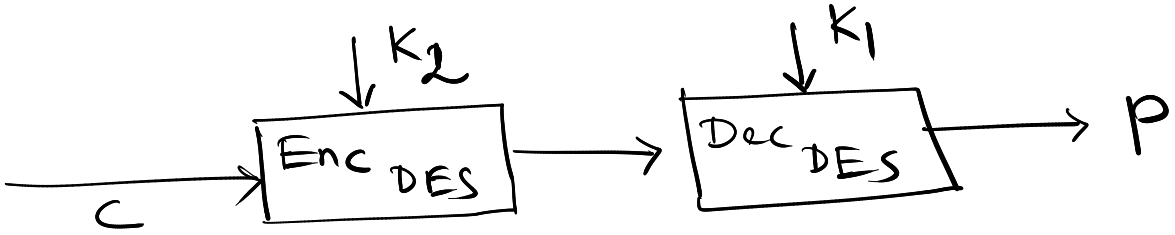

Dec




11) Enc




Dec




- EE , ED , DE , DD

$K = K_1 \| K_2$

Attacker knows plaintext $M$ and the corresponding ciphertext $C$

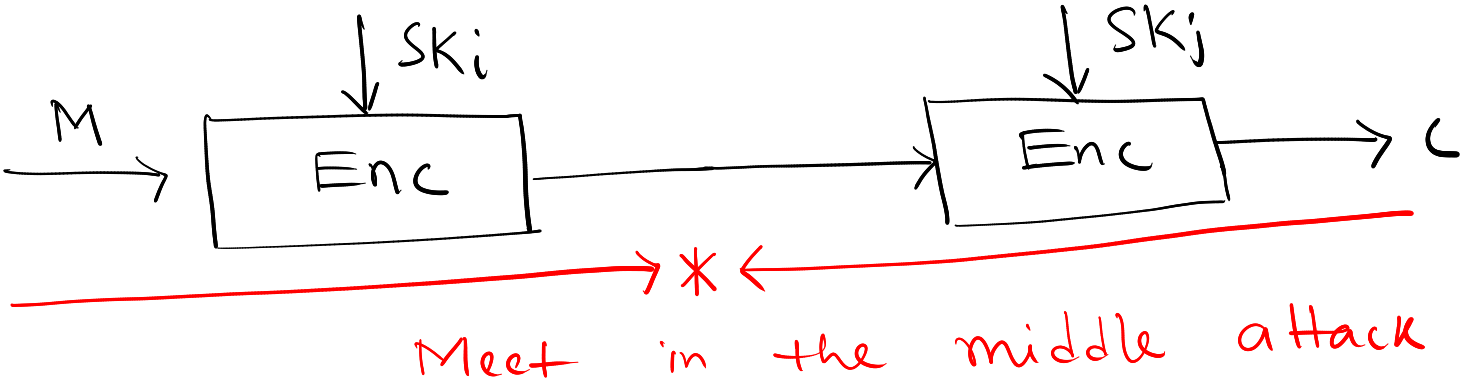
$$C = Enc\left(Enc(M, K_1), K_2\right)$$

$$Keys = \{SK_1, \ldots SK_{2^{56}}\}$$

$$Enc(M, SK_i) = X_i$$

$$Dec(C, SK_j) = Y_j$$

If $X_i = Y_j$ for some $i, j$ then the key is $SK_i \| SK_j$




$X_i$ $2^{56}$

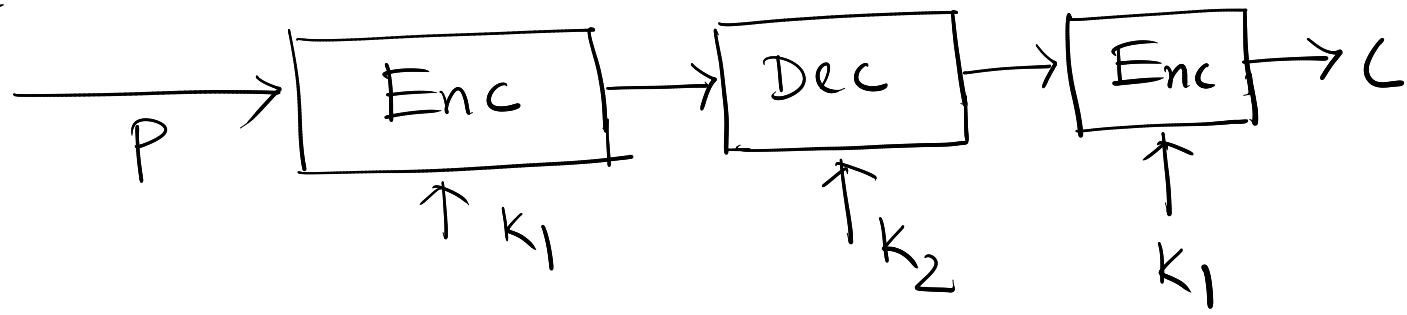
$Y_j$ $2^{56}$

## Triple Encryption

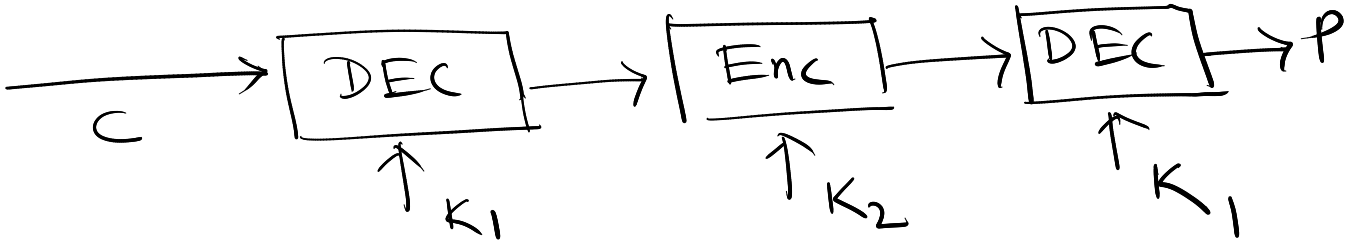
2n – bit security

$$K = K_1 \| K_2$$

1) Enc




Dec




- EEE, EDE, DED ---

- If DES is used in Triple encryption setup then it is known as Triple DES (3-DES)

---

- Advanced Encryption Standard (AES)

→ We have to understand Certain Mathematical results

A binary operation $*$ on a set $S$ is a mapping from $S \times S$ to $S$.
That is $*$ is a rule which assigns to each ordered pair of elements from $S$ to an element of $S$

$$* : S \times S \longrightarrow S$$

$$*(a,b) = c \quad , \quad a,b,c \in S$$

$$*(b,a) = d \qquad d \in c$$

it is not necessary that $d = c$

## Group

A group $(G, *)$ Consists of a set $G$ with a binary operation $*$ on $G$ Satisfying the following axioms

1) $*$ is associative on $G$

$$a * (b * c) = (a * b) * c \quad \forall\, a,b,c \in G$$

2) There is an element $e \in G$ Called the identity element Such that

$$a * e = a = e * a \quad \forall\, a \in G$$

3) For each $a \in G$ there exists an element $a^{-1} \in G$ Called the inverse of $a$ s.t.

$$a * a^{-1} = e = a^{-1} * a \quad \forall\, a \in G$$

☑ A group $G$ is called abelian (or commutative) if

$$a * b = b * a \quad \forall \; a, b \in G$$

---

Ex. $*$ : matrix multiplication over square matrices of order $n \times n$

$M$ : set of $n \times n$ matrices over $\mathbb{R}$

$(M, *) \rightarrow$ is it a Group ? (No)

a) $*$ is associative

$$A * (B * C) = (A * B) * C$$

b) $A * I_n = A = I_n * A$

c) $\forall \; A \in M \;\; \nexists \; A^{-1} \in M$ s.t

$$A * A^{-1} = I_n = A^{-1} * A$$

$M = \{$ Set of all invertible $n \times n$ matrix $\}$

$(M, *) \rightarrow$ Group

$(M, *) \rightarrow$ Commutative ?

$A * B \neq B * A$

not Commutative group

ex. $\mathbb{Z}$ : set of all integers

$(\mathbb{Z}, +)$ → Group ?

— yes

i) $a + (b + c) = (a + b) + c$

ii) $a + 0 = a = 0 + a \quad \forall a \in \mathbb{Z}$

iii) $\forall\ a \in \mathbb{Z} \quad \exists\ -a \in \mathbb{Z}$

s.t. $a + (-a) = 0 = (-a) + a$

---

ex. $(\mathbb{Z}, \times)$ → not a group

i) $a \times (b \times c) = (a \times b) \times c$

ii) $a \times 1 = a = 1 \times a$

iii) $a \in \mathbb{Z} \quad \nexists \quad a^{-1} \in \mathbb{Z}$

---

ex. $\mathbb{Q}$ : set of all rational numbers

$(\mathbb{Q}, \times)$ → not group

$(\mathbb{Q} \setminus \{0\}, \times)$ → group.

If $|G|$ is finite then $(G, *)$ is a finite group.

$|G|$: Cardinality of $G$

Ex. $(Z_n, +_n) \longrightarrow$ group

$Z_n = \{0, 1, 2, \cdots, n-1\}$

$x +_n y = (x+y) \bmod n$

Ex. $(Z_n \setminus \{0\}, *_n)$

$x *_n y = (x \cdot y) \bmod n$

$*_n$: multiplication modulo $n$.

i) $x *_n (y *_n z) = (x *_n y) *_n z$

$y *_n z = t \Rightarrow y \cdot z = d \cdot n + t$

$x *_n t \Rightarrow x \cdot y \cdot z = d_1 n \cdot + t_1$

2) $x *_n 1 = 1 *_n x = x$

3) $a *_n b = 1 = b *_n a$

$\forall a$

$a *_n b = 1$

$\Rightarrow a \cdot b = 1 + t \cdot n$

$\Rightarrow 1 = a \cdot b + t \cdot n$

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

* $\mathbb{Z}_n^* = \{ x \mid \gcd(x, n) = 1 \}$

$(\mathbb{Z}_n^*, *_n) \rightarrow$ group.

☒ A non empty subset $H$ of a group $(G, *)$ is subgroup of $G$ if $H$ is itself a group with respect to the same operation $*$ of $G$.

If $H$ is a proper subset of $G$ $(H \neq G, H \subset G)$ then $H$ is called a proper subgroup of $G$.

Check

i) $H \subseteq G$ or not

ii) $H$ is itself a group with $*$ or not

---

☒ $(G, *) \rightarrow$ group

$a \in G \Rightarrow a * a \in G \quad a * a = a^2$

$a * a * a \in G \quad a * a * a = a^3$

$a * a * \cdots * a$ ($i$ times) $\in G$

$a^i \in G$

$e$ = Identity element of $G$

$a^{\alpha} = e \Rightarrow \alpha$ (Smallest) is ($\alpha$: +ve integer)

called the order of $a$

$|G|$ : order of $G$.

- Group $\rightarrow (G, *)$ [G is closed under *]

$\boxed{\alpha \in G}$

$\alpha^0, \alpha^1, \alpha^2, \alpha^3, \ldots \in G$

$\downarrow$

Identity

for any $b \in G$

if $\exists\ i \geq 0$ s.t. $b = \alpha^i$

then $\alpha$ is called the generator of $(G, *)$

- $(G, *) = \langle \alpha \rangle$

- A group $G$ is cyclic if there is an element $\alpha \in G$ such that for every $b \in G$ there is an integer $i$ with $b = \alpha^i$. This $\alpha$ is called the generator of $G$

$$G = \langle \alpha \rangle$$

- $(G, *)$ $\quad |G|$ : finite

$o(a) = m$ , $a^m = e$

$a \in G$

$e = a^0, a^1, a^2, \ldots, a^{m-1} \in G$

$$H = \{e = a^0, a^1, a^2, \ldots a^{m-1}\}$$

i) $H \subseteq G$ ✓

ii) $H$ is group under $*$

if $x, y \in H$

$\Rightarrow x * y \in H$

for every $a^i \in H$ $\exists$ the inverse of $a^i$

H is group with $*$

H is a Subgroup of G

$$H = \langle a \rangle$$

H is a cyclic Subgroup of G.

$$|H| = |\langle a \rangle| \rightarrow \text{order of the cyclic Subgroup}$$

$$= o(a)$$

☒ Lagrange's theorem

If G is a finite group and H is a Subgroup of G then $|H|$ divides $|G|$

☒ $G$ is a finite group

$a \in G$

$o(a) \mid |G|$

$\Rightarrow$ $a \in G$ ,

$$H = \{ e = a^0, a^1, a^2, \cdots, a^{o(a)-1} \}$$

$H$ is a Subgroup of $G$

From Lagrange's theorem

$$|H| \mid |G|$$

$$\Rightarrow o(a) \mid |G|$$

---

☒ If the order of $a \in G$ is $t$

then $o(a^k) = \dfrac{t}{\gcd(t,k)}$

☒ If $\gcd(t,k) = 1$

then $o(a^k) = t = o(a)$

$$\Rightarrow |\langle a^k \rangle| = |\langle a \rangle|$$

$x \in \langle a^k \rangle$ $\qquad$ $\langle a \rangle$

$\Rightarrow x = (a^k)^i = a^{ki} \in \langle a \rangle$

$$\langle a^K \rangle \subseteq \langle a \rangle$$

$$\Rightarrow \quad \langle a^K \rangle = \langle a \rangle$$

> $a^K$ is also a generator of $\langle a \rangle$

$\langle a^K \rangle = \langle a \rangle$ Subgroup generated by $a$

$\langle a \rangle = \langle a^K \rangle$ subgroup generated by $a^K$

---

$$Z_{19}^* = \{ x \mid \gcd(x, 19) = 1, \ 1 \le x \le 18 \}$$

$*_{19}$ : multiplication modulo 19

$$x *_{19} y = (x \cdot y) \bmod 19$$

Find the generators of $(Z_{19}^*, *_{19})$

H.T

$\Rightarrow \quad x \in Z_{19}^*$

$S = \{ x^0, x^1, \dots \}$

## Ring

A ring $(R, +_R, \times_R)$ consists of one set $R$ with two binary operations arbitrarily denoted by $+_R$ (addition) and $\times_R$ (multiplication) on $R$ satisfying the following properties

i) $(R, +_R)$ is a abelian group with the identity element $0_R$

ii) The operation $\times_R$ is associative

i.e., $a \times_R (b \times_R c) = (a \times_R b) \times_R c \quad \forall\, a, b, c \in R$

iii) There is a multiplicative identity denoted by $1_R$ with $1_R \neq 0_R$ s.t.

- $1_R \times_R a = a \times_R 1_R = a \quad \forall\, a \in R$

iv) The operation $\times_R$ is distributive over $+_R$

i.e. $(b +_R c) \times_R a = (b \times_R a) +_R (c \times_R a)$

$a \times_R (b +_R c) = (a \times_R b) +_R (a \times_R c)$

Ex. $(Z, +, \cdot)$ : check it is Ring or not

H.T.

$Z \rightarrow$ set of all integers

---

- $(R, +_R, \times_R) \rightarrow$ Ring
  - $a \times_R b = b \times_R a \quad \forall\ a, b \in R$

  then $(R, +_R, \times_R)$ is a Commutative Ring

- $(Z, +, \cdot) \rightarrow$ Ring

  $\Rightarrow a \cdot b = b \cdot a \quad \forall\ a, b \in Z$

  Commutative Ring

- An element 'a' of a ring R is called unit or an invertible element if there is an element $b \in R$ s.t. $a \times_R b = 1_R$

☒ the set of units in a Ring R forms a group under multiplication operation.

⇒ This is known as group of units of R

---

☒ Field

A field is a nonempty set F together with two binary operation + (addition) and * (multiplication) for which the following properties are satisfied

i) $(F, +)$ is an abelian group

ii) If $0_F$ denotes the additive identity element of $(F, +)$ then $(F \setminus \{0_F\}, *)$ is a commutative/abelian group

iii) $\forall\ a, b, c \in F$ we have

$$a * (b + c) = (a * b) + (a * c)$$

ex. i) $(\mathbb{Z}, +, \cdot)$ → Not a field

ii) $(\mathbb{Q}, +, \cdot)$ → Field or not?

$(\mathbb{Q}, +)$ → abelian group

$0$ : additive identity

$1$ : multiplicative identity

$(\mathbb{Q} \setminus \{0\}, \cdot)$ : abelian group

$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

---

$p$ → prime number

$$\mathbb{F}_p = \{0, 1, 2, \cdots, p-1\}$$

$(\mathbb{F}_p, +_p, *_p)$ → Field or not?

$$x +_p y = (x + y) \bmod p$$

$$x *_p y = (x \cdot y) \bmod p$$

$x + y = t_1 P + r_1$

$z = t_1 P + r_2$

$= t_2 P + r_3$

$x + y + z = t_2 P + r_3$

i) $(\mathbb{F}_p, +_p) \rightarrow$ abelian group

ii) $(\mathbb{F}_p \setminus \{0\}, *_p)$

1 : Identity element (multiplicative)

$\forall\ a \in \mathbb{F}_p \setminus \{0\} \quad \exists\ b \in \mathbb{F}_p \setminus \{0\}$

s.t. $a *_p b = 1$

$\Rightarrow (a \cdot b) \bmod p = 1$

$(ab - 1) = t \cdot p$

$\Rightarrow 1 = a \cdot b + t_1 \cdot p$

$\boxed{\gcd(a, p) = a \cdot b + t_1 p}$

↓

Extended Eucledian Algo

## Field Extension

Suppose $K_2$ is a field with addition $(+)$ and multiplication $(*)$.

Suppose $K_1 \subseteq K_2$ is closed under both these operation such that $K_1$ it self is a field with the restriction of $+$ and $*$ to the set $K_1$

Then $K_1$ is called a Subfield of $K_2$ and $K_2$ is called a field extension of $K_1$.

---

$F \rightarrow$ field $(F, +, *)$

$$F[x] = \left\{ a_0 + a_1 x + a_2 x^2 + \cdots \;\middle|\; a_i \in F \right\}$$

↓

Polynomial ring

$$\left( F[x] , \underline{+} , \underline{*} \right)$$

$F \rightarrow$ field $\quad (F, +, *)$

$$F[x] = \{ a_0 + a_1 x + a_2 x^2 + \cdots \mid a_i \in F \}$$

$(F[x], +, *) \longrightarrow$ Polynomial Ring

$+$ : polynomial addition

$*$ : polynomial multiplication

$P_1(x) \in F[x] \qquad P_1(x) = a_0 + a_1 x + a_2 x^2$

$P_2(x) \in F[x] \qquad P_2(x) = b_0 + b_1 x + b_2 x^2$

$$P_1(x) + P_2(x) = (a_0 + a_1 x + a_2 x^2) + (b_0 + b_1 x + b_2 x^2)$$

$$= (a_0 + b_0) + (a_1 + b_1) x + (a_2 + b_2) x^2$$

$(a_i + b_i) \rightarrow$ Field addition

---

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$$

$$b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1} x^{n-1}$$

$+$

$$(a_0 + b_0) + (a_1 + b_1) x + (a_2 + b_2) x^2 + \cdots + (a_{n-1} + b_{n-1}) x^{n-1}$$

$(a_i + b_i)$ : additive operation on $F$ as $a_i, b_i \in F$

$$(a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}) * (b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1} x^{n-1})$$

$$= (a_0 * b_0) + (a_0 * b_1 + a_1 * b_0)\, x + \cdots + (a_{n-1} * b_{n-1})\, x^{2n-2}$$

$a_i * b_i \rightarrow$ Field multiplication in $F$ as $a_i, b_i \in F$

addition between the elements has to be done in the Field.

- $(F[x], +, *)$ is a polynomial ring

i) $(F[x], +)$ must be an abelian group

$$(a_0 + a_1 x + a_2 x^2) + (b_0 + b_1 x + b_2 x^2) \qquad a_i \in F$$

$$a_i + b_i = 0$$

$$(a_0 + b_0) + (a_1 + b_1)\, x + (a_2 + b_2)\, x^2 = 0$$

ii) $*$ is associative

iii) $1$ is the multiplicative identity

iv) $*$ is distributive over $+$

$\mathbb{F}_2 = \{0, 1\}$ $\quad (\mathbb{F}_2, +_2, *_2) \rightarrow$ Field.

$$\mathbb{F}_2[x] = \left\{ a_0 + a_1 x + a_2 x^2 + \cdots \mid a_i \in \mathbb{F}_2 \right\}$$

$P(x) = x + 1 \quad \in \mathbb{F}_2[x]$

$q(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$

$$P(x) + q(x) = (x+1) + (x^2 + x + 1)$$
$$= x^2 + (1+1)x + (1+1)$$
$$= x^2$$

$$P(x) * q(x) = (x+1) * (x^2 + x + 1)$$
$$= (x^3 + x^2 + x) + (x^2 + x + 1)$$
$$= x^3 + (1+1)x^2 + (1+1)x + 1$$
$$= x^3 + 1$$

---

A polynomial $P(x) \in F[x]$ of degree $n$ $(n \geq 1)$ is called irreducible if it cannot be written in the form of $P_1(x) * P_2(x)$ with $P_1(x), P_2(x) \in F[x]$ and degree of $P_1(x), P_2(x)$ must be $\geq 1$

$P(x) \neq P_1(x) * P_2(x)$

☒ $x^2+1 \in \mathbb{F}_2[x]$

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

$$(x^2+1) = (x+1)*(x+1) \text{ in } \mathbb{F}_2[x]$$

$x^2+1$ is reducible in $\mathbb{F}_2[x]$

---

☒ $I = \langle P(x) \rangle = \{ q(x) \cdot P(x) \mid q(x) \in F[x] \}$

$I \rightarrow$ ideal generated by $P(x)$

☒ $F[x] / \langle P(x) \rangle$

$q(x) \in F[x]$ $\quad \boxed{deg(r(x)) < deg(P(x))}$

$$q(x) = d(x) * P(x) + r(x)$$

$r(x) \in F[x] / \langle P(x) \rangle$

If $P(x)$ is irreducible polynomial then $\left( F[x]/\langle P(x) \rangle , + , * \right)$ becomes a field.

$F[x] / \langle p(x) \rangle$

$\rightarrow$ contains Polyn of degree $< \deg(p(x))$

---

$x^2 + x + 1 \in \mathbb{F}_2[x]$ , $\mathbb{F}_2 = \{0, 1\}$

$p(x) = x^2 + x + 1$ is irreducible.

* $\mathbb{F}_2[x] / \langle x^2 + x + 1 \rangle$

$$q(x) = d(x) \cdot p(x) + r(x)$$

$$\deg(r(x)) < 2$$

$$r(x) \in \{0, 1, x, x+1\}$$

$$x^2 + x + 1 \;\big)\; x^2 + 1 \;\big(\; 1$$
$$x^2 + x + 1$$
$$x$$

$$x^2 + 1$$
$$x^2 + x + 1$$
$$x^2 + 1 \rightarrow x + 1$$

- $x^2 + 1$

$x^2 = x + 1$

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

$$x^2 + x + 1 \;\big)\; x^3 + 1 \;\big(\; x + 1$$
$$x^3 + x^2 + x$$
$$x^2 + x + 1$$
$$x^2 + x + 1$$
$$0$$

$$x^3+1 = x\cdot x^2+1$$
$$= x\cdot(x+1)+1$$
$$= x^2+x+1$$
$$= (x+1)+(x+1)$$
$$= 0$$

$x^2+1 \overline{)\, x^2+1 \,(\, 1}$
$x^2+1$
$\overline{0}$

$x^2 = 1$

$x^2+1$
$= 1+1$
$= 0$

$x^2+x+1 \;\Big)\; g(x) \;($

$$g(x) = d(x)\cdot(x^2+x+1)+r(x)$$

---

$$\mathbb{F}_2[x] \Big/ \langle x^2+x+1 \rangle$$

$x^2+x+1 = 0$

$\alpha$ is the root of $x^2+x+1=0$

$\alpha^2+\alpha+1 = 0$

$\Rightarrow \alpha^2 = \alpha+1$

$\langle \alpha \rangle$

$o(\alpha) = 2$

$\{0, 1=\alpha^0, \alpha^1, \alpha^2 = \alpha+1\} =$

$\Rightarrow \{0, 1, \alpha, \alpha+1\}$

$\alpha^3 = \alpha\cdot\alpha^2$
$= \alpha(\alpha+1)$
$= \alpha^2+\alpha$
$= 1$

$\{0, 1, \alpha, \alpha+1\} \rightarrow \{0, 1, x, x+1\}$

$\mathbb{F}_2[x] / \langle x^2 + x + 1 \rangle$

→ all such poly$^n$ of deg $< 2$

$x^2 + x + 1$ → is know as primitive poly$^n$.

# Advanced Encryption Standard (AES)

It is Standardized by NIST

- Rijndael
  Winner of Advanced Encryption Standard Competition.
- Winner of Competition was named as AES

AES → i) Iterated block cipher

ii) It is based on SPN

## AES-128

i) Block Size = 128 bit

ii) Number of rounds = 10

iii) Secret key Size = 128 bit

## AES-192

i) Block Size = 128 bit

ii) Number of rounds = 12

iii) Secret Key Size = 192 bit

## AES-256

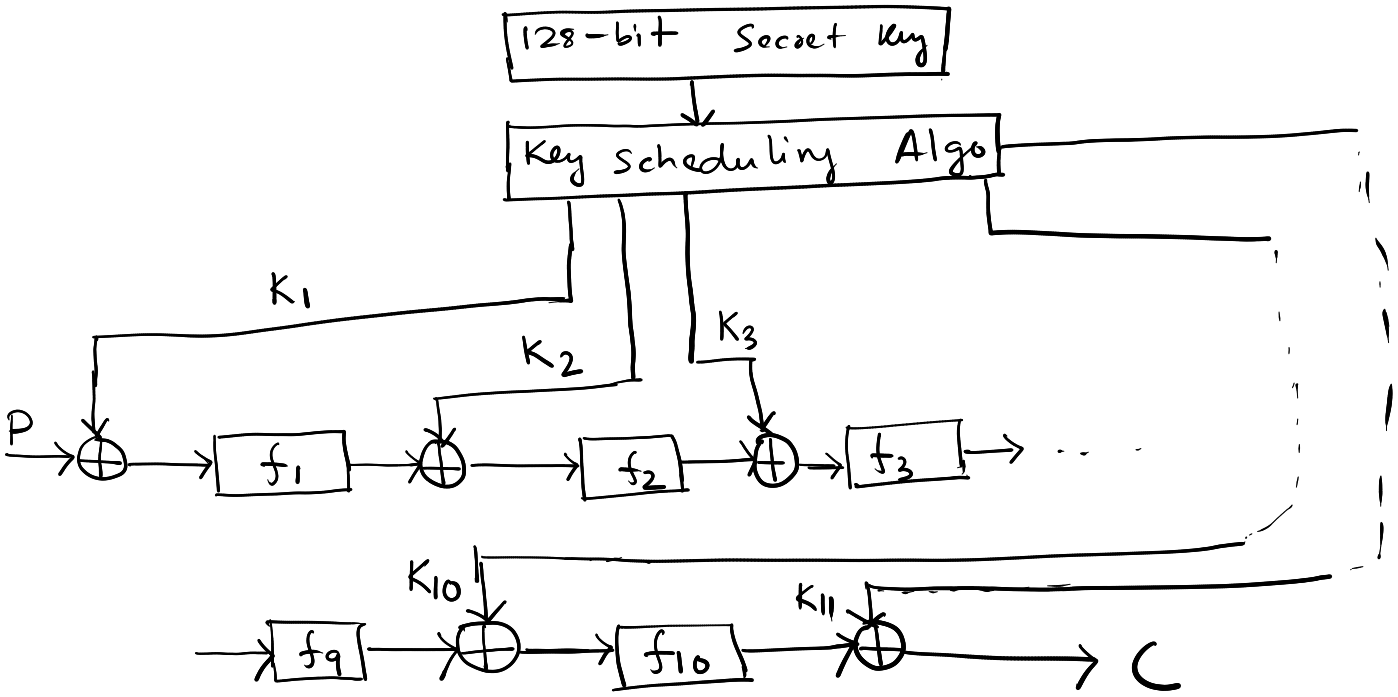
i) Block Size = 128 bit

ii) Number of rounds = 14

iii) Secret Key Size = 256 bit

---

## AES-128




P → plaintext block = 128 bit

C → Ciphertext block = 128 bit

Ki → round keys = 128 bit

- We have to understand the followings:
  - i) Round functions
  - ii) Key scheduling Algo

- **Round functions of AES-128**

$f_1, f_2, \ldots, f_{10}$

i) $f_1 = f_2 = f_3 \ldots = f_9$

ii) $f_{10}$ is different from $f_i$, $i = 1, \ldots 9$

First 9 round functions are exactly same
10 th round function is different from other 9 round function

- The first 9 round functions (i.e., $f_1, \ldots f_9$) are based on the following functions

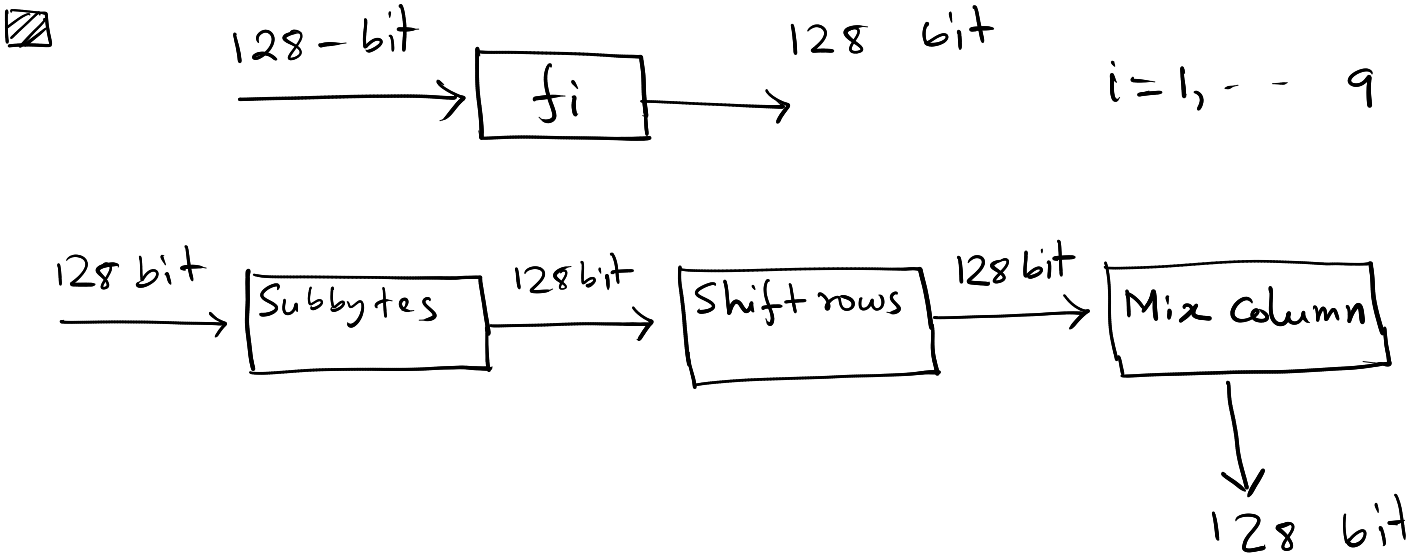
$$f_i : \{0,1\}^{128} \longrightarrow \{0,1\}^{128}$$

  - i) Subbytes
  - ii) Shift rows
  - iii) Mix Column

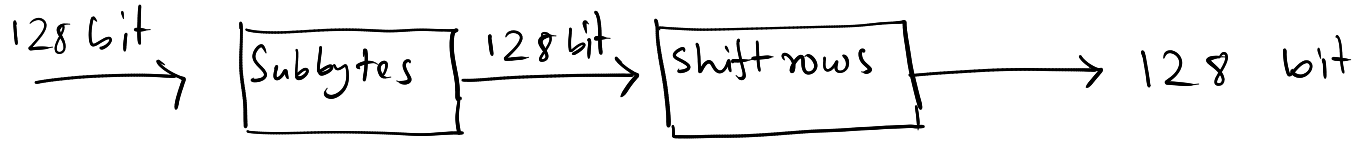
The 10-th round function (i.e., $f_{10}$) is based on

$$f_{10} : \{0,1\}^{128} \longrightarrow \{0,1\}^{128}$$

  - i) Subbytes
  - ii) Shift rows




For 10 th round




---

## Subbytes

$$\text{Subbytes} : \{0,1\}^{128} \longrightarrow \{0,1\}^{128}$$

$\$ \longrightarrow$ Input

$$\$ \longrightarrow \begin{bmatrix} \$_{00} & \$_{01} & \$_{02} & \$_{03} \\ \$_{10} & \$_{11} & \$_{12} & \$_{13} \\ \$_{20} & \$_{21} & \$_{22} & \$_{23} \\ \$_{30} & \$_{31} & \$_{32} & \$_{33} \end{bmatrix}_{4\times4} \qquad \$_{ij} \rightarrow 8 \text{ bit}$$

---

P → plainteat 128 bit

$P = P_0 P_1 \cdots P_{15}$ $\quad len(P_i) = 8$ bit

$$P \rightarrow \begin{bmatrix} P_0 & P_4 & P_8 & P_{12} \\ P_1 & P_5 & P_9 & P_{13} \\ P_2 & P_6 & P_{10} & P_{14} \\ P_3 & P_7 & P_{11} & P_{15} \end{bmatrix} \oplus K_1 \rightarrow \begin{bmatrix} \$_{00} & \$_{01} & \$_{02} & \$_{03} \\ \$_{10} & \$_{11} & \$_{12} & \$_{13} \\ \$_{20} & \$_{21} & \$_{22} & \$_{23} \\ \$_{30} & \$_{31} & \$_{32} & \$_{33} \end{bmatrix}$$

## Subbytes

$$\$ = (s_{ij})_{4\times 4}$$

- $S : \{0,1\}^8 \longrightarrow \{0,1\}^8$ $\qquad S(0) = 0$

i) $(c_7 c_6 c_5 c_4 c_3 c_2 c_1 c_0) = (01100011)$

ii) $S(s_{ij}) = (a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0)$

iii) For $i = 0$ to $7$

$$b_i = (a_i + a_{(i+4)\%8} + a_{(i+5)\%8} + a_{(i+6)\%8} + a_{(i+7)\%8} + c_i) \bmod 2$$

iv) $(b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0)$

v) $s'_{ij} = (b_7 b_6 \cdots b_0)$

$$\begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} \longrightarrow \begin{bmatrix} s'_{00} & s'_{01} & s'_{02} & s'_{03} \\ s'_{10} & s'_{11} & s'_{12} & s'_{13} \\ s'_{20} & s'_{21} & s'_{22} & s'_{23} \\ s'_{30} & s'_{31} & s'_{32} & s'_{33} \end{bmatrix}$$

128 bit $\qquad$ 128 bit

We have to learn $S : \{0,1\}^8 \longrightarrow \{0,1\}^8$

$P \rightarrow P_0 P_1 \cdots P_{15}$ $\quad len(P_i) = 8$ bit

$$\begin{pmatrix} P_0 & P_4 & \cdots & P_{12} \\ P_1 & \vdots & & P_{13} \\ P_2 & \cdots & & P_{14} \\ P_3 & P_7 & & P_{15} \end{pmatrix} \oplus K_1 = (s_{ij})_{4\times 4}$$

$$S : \{0,1\}^8 \longrightarrow \{0,1\}^8$$

$$S(s_{ij}) = (a_7 \cdots a_0)$$

$$(c_7, \cdots c_0)$$

$$(b_7 \cdots b_0)$$

$$S : \{0,1\}^8 \longrightarrow \{0,1\}^8$$

$S(0) = 0$ $\quad a_i \in \mathbb{F}_2$

$X \neq 0 \in \{0,1\}^8$

$S(X) = Y \in \{0,1\}^8$

$X = (a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0)$ , $a_i \in \{0,1\}$

$$P(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7$$

$deg(P(x)) \leq 7$

$P(x) \in \mathbb{F}_2[x]$

$(\mathbb{F}_2[x], +, *)$

- $g(x) = x^8 + x^4 + x^3 + x + 1$ $g(x)$ is a primitive polynomial

$$\left( \frac{F_2[x]}{\langle g(x) \rangle}, +, * \right) \rightarrow \text{Field}$$

Find the multiplicative inverse of $P(x)$ under modulo $(x^8 + x^4 + x^3 + x + 1)$

$$P(x) \cdot q(x) \equiv 1 \mod (x^8 + x^4 + x^3 + x + 1)$$

$$\Rightarrow P(x) \cdot q(x) - 1 = h(x) \cdot (x^8 + x^4 + x^3 + x + 1)$$

$$\Rightarrow 1 = P(x) \cdot q(x) + h_1(x) \cdot (x^8 + x^4 + x^3 + x + 1)$$

$$gcd(a, b) = a \cdot s + b \cdot t$$

$$gcd(P(x), x^8 + x^4 + x^3 + x + 1) = 1$$

How to find $q(x)$ ?

$\Rightarrow$ Extended Eucledian Algo finds $q(x)$

$q(x) \rightarrow$ polyn of degree atmost 7

$$q(x) = r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4 + r_5 x^5 + r_6 x^6 + r_7 x^7$$

$$q(x) \rightarrow (r_7 r_6 r_5 \cdots r_0) \in \{0,1\}^8$$

$$S(X) = Y = (r_7 r_6 \cdots r_0)$$

**Ex** Find

$S(01010011) = ?$ $\quad X = (01010011)$, $P(x)$

$P(x) = x^6 + x^4 + x + 1$

$g(x) = x^8 + x^4 + x^3 + x + 1$

$$x^6 + x^4 + x + 1 \;\Big)\; x^8 + x^4 + x^3 + x + 1 \;\Big(\; x^2 + 1$$
$$x^8 + x^6 + x^3 + x^2$$
$$x^6 + x^4 + x^2 + x + 1$$
$$x^6 + x^4 + x + 1$$

$$x^2 \;\Big)\; x^6 + x^4 + x + 1 \;\Big(\; x^4 + x^2$$
$$x^6$$
$$x^4 + x + 1$$
$$x^4$$

$$x + 1 \;\Big)\; x^2 \;\Big(\; x + 1$$
$$x^2 + x$$
$$x$$
$$x + 1$$
$$1$$

$$1 = x^2 + (x+1)(x+1)$$
$$= x^2 + (x+1)\left[(x^6 + x^4 + x + 1) + x^2(x^4 + x^2)\right]$$
$$= (x+1)(x^6 + x^4 + x + 1) + \left[1 + (x+1)(x^4 + x^2)\right] x^2$$

$$= (x+1)(x^6 + x^4 + x + 1) + (1 + x^5 + x^3 + x^4 + x^2) \cdot x^2$$

$$= (x+1)(x^6 + x^4 + x + 1) + (1 + x^5 + x^4 + x^3 + x^2)\Big[(x^8 + x^4 + x^3 + x + 1) + (x^2+1)(x^6 + x^4 + x + 1)\Big]$$

$$= (1 + x^5 + x^4 + x^3 + x^2)(x^8 + x^4 + x^3 + x + 1) + \Big[(x+1) + (1 + x^5 + x^4 + x^3 + x^2)(x^2+1)\Big](x^6 + x^4 + x + 1)$$

$$= h_1(x) \cdot g(x) + (x+1 + x^2 + x^7 + x^6 + x^5 + x^4 + 1 + x^5 + x^4 + x^3 + x^2)(x^6 + x^4 + x + 1)$$

$$= h_1(x) \cdot g(x) + (x^7 + x^6 + x^3 + x)(x^6 + x^4 + x + 1)$$

$$\Rightarrow 1 = h_1(x) \cdot g(x) + (x^7 + x^6 + x^3 + x)(x^6 + x^4 + x + 1)$$

$$q(x) = x^7 + x^6 + x^3 + x$$

which is the multiplicative inverse of $(x^6 + x^4 + x + 1)$

- $S(01010011) = (11001010)$

$= (a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0)$

$c = (01100011)$

$$b_i = (a_i + a_{(i+4)\%8} + a_{(i+5)\%8} + a_{(i+6)\%8} + a_{(i+7)\%8} + c_i) \bmod 2$$

$$b_0 = (a_0 + a_4 + a_5 + a_6 + a_7 + c_0) \bmod 2$$
$$= (0+0+0+1+1+1) \bmod 2$$
$$= 1$$

$b_1 = 0$

$(b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0)$

$= (11101101)$

Subbytes $(0101\ 0011) = (1110\ 1101)$

$0101$: 5, $0011$: 3; $1110$: E, $1101$: D

Subbytes $(5\ 3) = ED$

Input $= (XY)$

Subbyte (Input) = element present in the row number $X$ and column number $Y$

Table is available in the Stinson book PP — 112

## Shift rows

Shiftrows : $\{0,1\}^{128} \longrightarrow \{0,1\}^{128}$

$$\begin{matrix} 0 \\ 1 \\ 2 \\ 3 \end{matrix} \begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} \longrightarrow \begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{11} & s_{12} & s_{13} & s_{10} \\ s_{22} & s_{23} & s_{20} & s_{21} \\ s_{33} & s_{30} & s_{31} & s_{32} \end{bmatrix}$$

## Mix Column

Mix column : $\{0,1\}^{128} \longrightarrow \{0,1\}^{128}$

$$(s_{ij})_{4\times 4} \longrightarrow (s'_{ij})_{4\times 4}$$

Consider the column $c \in \{0,1,2,3\}$

$$\text{Column} = \begin{pmatrix} s_{0c} \\ s_{1c} \\ s_{2c} \\ s_{3c} \end{pmatrix}$$

$s_{ic} = (a_7 a_6 \cdots a_0)$

$\text{Poly}^n = a_0 + a_1 x + \cdots + a_7 x^7$

For $i = 0$ to $3$

$t_i = \text{Binary to poly}\ (s_{ic})$

$$u_0 = \left[(x * t_0) + (x+1) * t_1 + t_2 + t_3\right] \bmod \left(x^8 + x^4 + x^3 + x + 1\right)$$

$$u_1 = \left[(x * t_1) + (x+1) * t_2 + t_3 + t_0\right] \bmod \left(x^8 + x^4 + x^3 + x + 1\right)$$

$$u_2 = \left[ (x * t_2) + (x+1) * t_3 + t_0 + t_1 \right] \bmod \left( x^8 + x^4 + x^3 + x + 1 \right)$$

$$u_3 = \left[ (x * t_3) + (x+1) * t_0 + t_1 + t_2 \right] \bmod \left( x^8 + x^4 + x^3 + x + 1 \right)$$

- $s'_{ic}$ = polynomial to binary $(u_i)$

$$\begin{pmatrix} s_{0c} \\ s_{1c} \\ s_{2c} \\ s_{3c} \end{pmatrix} \xrightarrow{\text{mix column}} \begin{pmatrix} s'_{0c} \\ s'_{1c} \\ s'_{2c} \\ s'_{3c} \end{pmatrix}$$

Mix Column

$$\begin{bmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{bmatrix} * \begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix}$$

$$\bmod \left( x^8 + x^4 + x^3 + x + 1 \right) = (s'_{ij})_{4\times 4}$$

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * (s_{ij}) \bmod (\cdot) = (s'_{ij})_{4\times 4}$$

$$x \longrightarrow (0\ 0000010) = 2$$

$$x+1 \longrightarrow (0\ 0000011) = 3$$

Find $\begin{bmatrix} s'_{00} \\ s'_{10} \\ s'_{20} \\ s'_{30} \end{bmatrix}$ after doing mixcolumn operation on $\begin{bmatrix} s_{00} \\ s_{10} \\ s_{20} \\ s_{30} \end{bmatrix}$

where $s_{00} = 95$, $s_{10} = 65$, $s_{20} = FD$

$s_{30} = F3$

$\Rightarrow s_{00} = 95 = 10010101 = x^7 + x^4 + x^2 + 1$

$s_{10} = 65 = 01100101 = x^6 + x^5 + x^2 + 1$

$s_{20} = FD = 11111101 = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$

$s_{30} = F3 = 11110011 = x^7 + x^6 + x^5 + x^4 + x + 1$

$s'_{00} = (x \times s_{00}) + ((x+1) \times s_{10}) + s_{20} + s_{30}$

$x \times s_{00} = x \times (x^7 + x^4 + x^2 + 1)$

$= x^8 + x^5 + x^3 + x \mod (x^8 + x^4 + x^3 + x + 1)$

$(x \times s_{00}) \mod (x^8 + x^4 + x^3 + x + 1)$

$= (x^8 + x^5 + x^3 + x) \mod (x^8 + x^4 + x^3 + x + 1)$

$x^8 + x^4 + x^3 + x + 1 \;\big)\; x^8 + x^5 + x^3 + x \;\big(\; 1$

$x^8 + x^4 + x^3 + x + 1$

$x^5 + x^4 + 1$

$$x^8 + x^5 + x^3 + x \equiv (x^4 + x^3 + x + 1) + x^5 + x^3 + x$$

$$\equiv x^5 + x^4 + 1 \mod (x^8 + x^4 + x^3 + x + 1)$$

$$x * S_{00} = x^5 + x^4 + 1$$

$$(x+1) * S_{10} = (x+1) * (x^6 + x^5 + x^2 + 1)$$

$$= x^7 + x^6 + x^3 + x + x^6 + x^5 + x^2 + 1$$

$$= x^7 + x^5 + x^3 + x^2 + x + 1$$

$$S'_{00} = (x * S_{00}) + (x+1) * S_{10} + S_{20} + S_{30}$$

$$= (x^5 + x^4 + 1) + (x^7 + x^5 + x^3 + x^2 + x + 1)$$

$$+ (x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1)$$

$$+ (x^7 + x^6 + x^5 + x^4 + x + 1)$$

$$= x^7 + x^4$$

$$S'_{00} = x^7 + x^4 = (10010000)$$

$$= 90$$

$S'_{10} = ?$

$S'_{20} = ?$

$S'_{30} = ?$

H.T

$$S'_{10} = \left((x * S_{10}) + (x+1) * S_{20} + S_{30} + S_{00}\right) \mod (x^8 + x^4 + x^3 + x + 1)$$

i) Subbytes

ii) Shiftrows

iii) Mix column

We are having clear idea on the round function

$f_1, f_2, \ldots f_9, f_{10}$

## Key scheduling

Input : 128 bit key

Output : 11 round keys

length of each round key is 128 bit

## Key scheduling Algo of AES-128

Input: 128 bit key

Output: 11 round keys, each of length 128 bit.

$$Key = (Key[15], \cdots, Key[0])$$

16 bytes

We will prepare 44 words which are denoted by $w[0], \cdots w[43]$

- $ROTWORD(B_0, B_1, B_2, B_3) = (B_1, B_2, B_3, B_0)$

- $SUBWORD(B_0, B_1, B_2, B_3) = (B_0', B_1', B_2', B_3')$

where $B_i' = SUBBYTES(B_i) \quad \forall i = 0, \cdots 3$

- 10 round constants (word)

$Rcon[1] = 01\,000000$

$Rcon[2] = 02\,00\,0000$

$Rcon[3] = 04\,00\,0000$

$Rcon[4] = 08\,00\,0000$

$Rcon[5] = 10\,00\,0000$

$Rcon[6] = 20\,00\,0000$

Rcon[7] = 40 000000

Rcon[8] = 80 000000

Rcon[9] = 1B 00 0000

Rcon[10] = 36 00 0000

for i = 0 to 3

$$W[i] = (Key[4i], Key[4i+1], Key[4i+2], Key[4i+3])$$

for i = 4 to 43

temp = W[i-1]

if $i \equiv 0 \bmod 4$

temp = SUBWORD(ROTWORD(temp)) ⊕ Rcon[i/4]

$$W[i] = W[i-4] \oplus temp$$

Return (W[0], ... W[43])

Round keys $K_1, K_2, \ldots, K_{11}$

$K_1 = W[0] \| W[1] \| W[2] \| W[3]$

$K_2 = W[4] \| W[5] \| W[6] \| W[7]$

⋮

$K_{11} = W[40] \| W[41] \| W[42] \| W[43]$

## Modes of operation

- I) ECB (Electronic Codebook mode)
  II) CFB (Cipher feedback mode)
- III) CBC (Cipher block chaining mode)
  IV) OFB (output feedback mode)
  V) Counter mode
  VI) CCM (Counter with Cipher block chaining mode)

## ECB

$$M = m_0 \| m_1 \| \cdots \| m_t$$

Enc → It can encrypt $l$ bit plaintext block

$$\text{len}(m_i) = l \text{ bit}$$

### Encryption

$$C = C_0 \| C_1 \| \cdots \| C_t$$

$$C_i = \text{Enc}(m_i, K) \quad \forall \; i = 0, \cdots, t$$

### Decryption

$$M = m_0 \| m_1 \| \cdots \| m_t$$

$$m_i = \text{Dec}(C_i, K) \quad \forall \; i = 0, \cdots t$$

Adv. Can be implemented parallely

Dis Adv: if $m_i = m_j$

then $c_i = c_j$

## CBC mode

$$M = m_1 \| m_2 \| \cdots \| m_t$$

Initialization vector = IV (Public variable)

Enc → block size $l$

$len(m_i) = l$

$len(IV) = l$

### Encryption

I) $c_0 = IV$

$$c_i = Enc(c_{i-1} \oplus m_i, K) \quad \forall\ i = 1, \cdots t$$

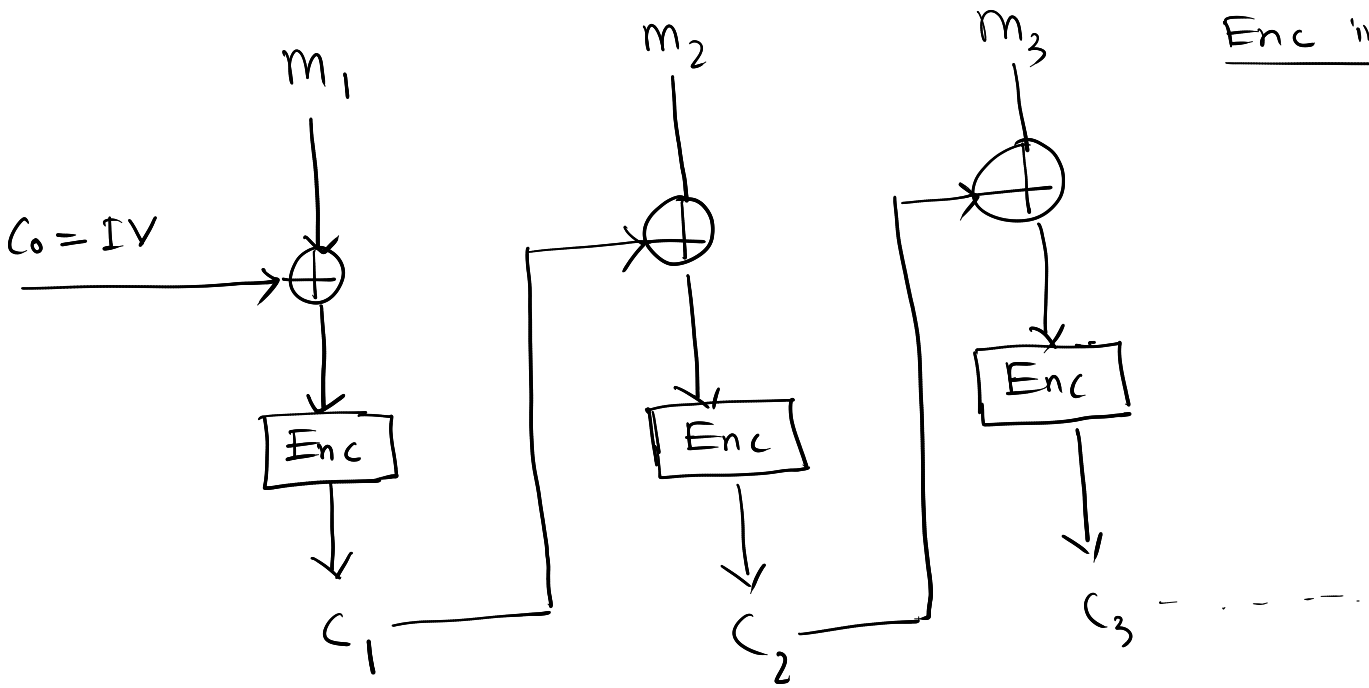
Ciphertext

$$C = c_0 \| c_1 \| c_2 \cdots \| c_t$$

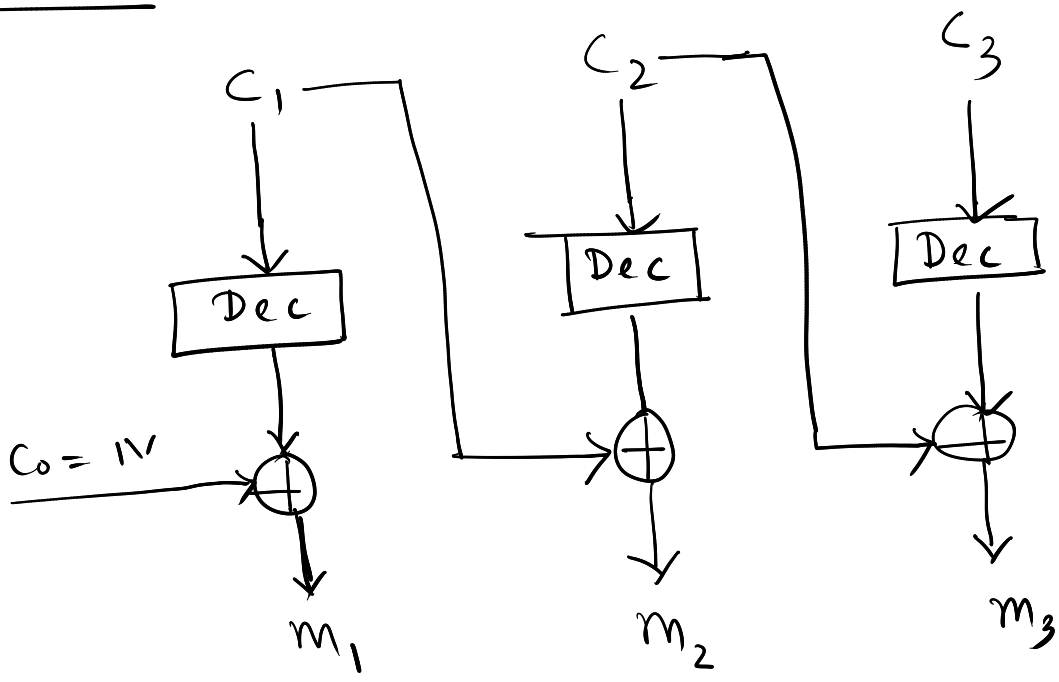
II) $$m_i = Dec(c_i, K) \oplus c_{i-1} \quad \forall\ i = 1, \cdots t$$

where $c_0 = IV$

Enc in CBC




Dec in CBC




- Other modes of operation can be found in Stinson's book

- Hash function

## Hash Function

$h : A \longrightarrow B$

$h(x) = Y$

i) If $x$ is altered to $x'$ then $h(x')$ will be completely different from $h(x)$

ii) Given $Y$ it is practically infeasible to find $X$ s.t. $h(x) = Y$

iii) Given $x$ and $y = h(x)$ it is practically infeasible to find $x'$ s.t. $h(x) = h(x')$

| Alice | | Bob |
|---|---|---|
| $X$ | $\xrightarrow{\quad X \quad}$ | $X_1$ |
| $S_1 = h(X, K)$ | $\xrightarrow{\quad S_1 \quad}$ | $S_2$ |

If $h(X_1, K) = S_2$

then Bob accept $X_1$

* We are able to check
  i) whether $X$ is altered during Communication
  ii) whether $S_1$ is " " Communication.

## Defⁿ

A hash family is a four tuple $(P, S, K, H)$ where the following conditions are satisfied

i) P is the set of all possible messages

ii) S is the set of all possible message digests or authentication tags

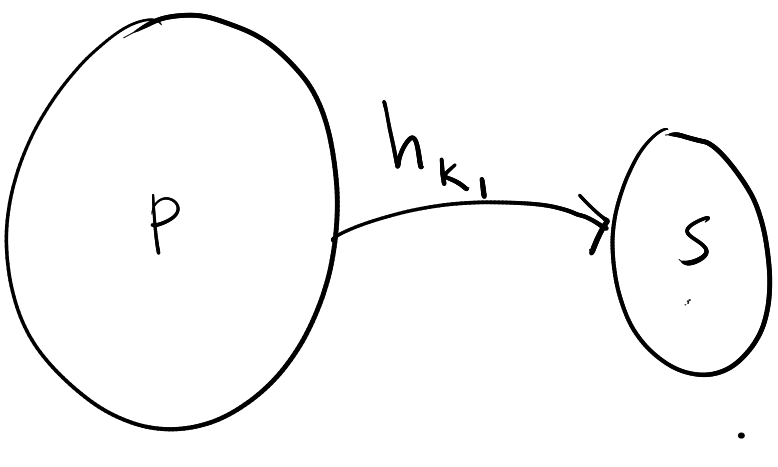
iii) K is the key space

iv) For each $K_1 \in K$ there is a hash function $h_{K_1} \in H$ s.t.

$$h_{K_1} : P \longrightarrow S$$

Here $|P| \geq |S|$

More interestingly $|P| \geq 2 \times |S|$




H : set of all hash functions

$h_{K_1}$ : hash function.

- If Key is involved in the Computation of hashed value then that hash function is Known as Keyed hash function

If Key is not required to Compute the hashed value then that hash function is Known as Unkeyed hash function.

---

- Problem 1

$$h : P \longrightarrow S$$

- Given $y \in S$ Find $x \in P$ such that $h(x) = y$

This problem is Known as preimage finding problem.

For an hash function h if you Can not find preimage in a feasible time then h is Known as preimage resistant hash function.

* Finding preimage is Computationally hard for preimage resistant hash function.

## Problem 2

$$h : P \longrightarrow S$$

Given $x \in P$ and $h(x)$ find $x' \in P$ s.t. $x' \neq x$ and $h(x') = h(x)$

This problem is Known as Second pre image finding problem.

If finding second preimage is Computationally hard for h then h is Known as Second preimage resistant hash function.

## Problem 3

$$h : P \longrightarrow S$$

Find $x, x' \in P$ s.t. $x \neq x'$ and $h(x) = h(x')$

This problem is Known as Collison finding problem.

For an hash function h if finding Collison is computationally hard then h is Known as Collison resistant hash function.

## Ideal Hash function

Let $h : P \longrightarrow S$ be an hash function.

$h$ will be called ideal hash function if given $x \in P$ to find $h(x)$ either you have to apply $h$ on $x$ or you have to look into the table corresponding to $h$ (hash table).

---

## Pre image finding Algorithm

$$h : X \longrightarrow Y$$

Choose any $X_0 \subseteq X$ s.t. $|X_0| = Q$

for each $x \in X_0$

Compute $y_x = h(x)$

if $y_x = y$

return $x$

- Pr [ the above algorithm returns Correct preimage ] $\Longrightarrow$ give you the complexity.

## Pre image finding Algo

Given $y \in Y$
find $x \in X$
s.t. $h(x) = y$

$h: X \longrightarrow Y$ ; $|Y| = M$

Choose any $X_0 \subseteq X$ s.t. $|X_0| = Q$

for each $x \in X_0$

Compute $y_x = h(x)$

if $y_x = y$

return $x$

$$X_0 = \{x_1, x_2, \ldots, x_Q\}$$

$E_i$ : event $h(x_i) = y$ ; $1 \le i \le Q$

$$Pr[E_i] = \frac{1}{M}$$

$$Pr[E_i^c] = 1 - \frac{1}{M}$$

$$Pr[E_1 \cup E_2 \cup E_3 \cup \ldots \cup E_Q]$$

$$= 1 - Pr[E_1^c \cap E_2^c \cap E_3^c \cap \ldots \cap E_Q^c]$$

$$= 1 - \prod_{i=1}^{Q} Pr[E_i^c]$$

$$= 1 - \left(1 - \frac{1}{M}\right)^Q$$

$$= 1 - \left[1 - \binom{Q}{1}\frac{1}{M} + \binom{Q}{2}\frac{1}{M^2} - \cdots\right]$$

$$\simeq 1 - \left[1 - \binom{Q}{1}\frac{1}{M}\right]$$

$$= \frac{Q}{M}$$

$$\Pr[\text{Pre image finding}] \simeq \frac{Q}{M}$$

Complexity of finding preimage $= O(M)$

---

## Collison finding Algo

$h : X \longrightarrow Y \qquad |Y| = M$

Find $x, x' \in X$ s.t. $x \neq x'$

and $h(x) = h(x')$

$X_0 \subseteq X \quad , |X_0| = Q$

$X_0 = \{x_1, \cdots x_Q\}$

for each $x \in X_0$

Compute $y_x = h(x)$

if $y_x = y_{x'}$ for some $x \neq x'$

then return $(x, x')$

else return failure

$E_i$ : event $h(x_i) \notin \{h(x_1), h(x_2), \ldots, h(x_{i-1})\}$

$X_0 = \{x_1, \ldots x_q\}$

$Pr[E_1] = 1$

$E_2$ : $h(x_2) \notin \{h(x_1)\}$

$h(x_2) = z$

$z \in Y \setminus \{h(x_1)\}$

$$Pr[E_2 | E_1] = \frac{M-1}{M}$$

$$\Rightarrow \frac{Pr[E_1 \cap E_2]}{Pr[E_1]} = \frac{M-1}{M}$$

$$\Rightarrow Pr[E_1 \cap E_2] = \frac{M-1}{M} \times Pr[E_1]$$

$$= \frac{M-1}{M}$$

$$Pr[E_3 \mid E_1 \cap E_2] = \frac{M-2}{M}$$

$$\Rightarrow \frac{Pr[E_1 \cap E_2 \cap E_3]}{Pr[E_1 \cap E_2]} = \frac{M-2}{M}$$

$$\Rightarrow Pr[E_1 \cap E_2 \cap E_3] = \frac{M-2}{M} \times Pr[E_1 \cap E_2]$$

$$= \frac{M-2}{M} \times \frac{M-1}{M}$$

$$Pr\left[E_4 \mid E_1 \cap E_2 \cap E_3\right] = \frac{M-3}{M}$$

$$\Rightarrow Pr\left[E_1 \cap E_2 \cap E_3 \cap E_4\right] = \frac{M-1}{M} \times \frac{M-2}{M} \times \frac{M-3}{M}$$

Continuing this process

$$Pr\left[E_1 \cap E_2 \cap E_3 \cdots \cap E_Q\right]$$

$$= \frac{M-1}{M} \times \frac{M-2}{M} \times \frac{M-3}{M} \cdots \times \frac{M-(Q-1)}{M}$$

$$Pr\left[\text{Collison finding Algo return Success}\right]$$

$$= 1 - Pr\left[E_1 \cap E_2 \cap E_3 \cdots \cap E_Q\right]$$

$$= 1 - \left[\frac{M-1}{M} \times \frac{M-2}{M} \times \cdots \times \frac{M-(Q-1)}{M}\right]$$

$$e^{-x} = 1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} + \cdots$$

$$\simeq 1 - x$$

$$\frac{M-i}{M} = 1 - \frac{i}{M}$$

$$\simeq e^{-\frac{i}{M}}$$

$$\frac{M-1}{M} \times \frac{M-2}{M} \times \cdots \times \frac{M-(Q-1)}{M}$$

$$\simeq \prod_{i=1}^{Q-1} e^{-\frac{i}{M}}$$

$$= e^{-\sum_{i=1}^{Q-1} \frac{i}{M}}$$

$$= e^{-\frac{1}{M} \sum_{i=1}^{Q-1} i}$$

$$= e^{-\frac{1}{M} \frac{(Q-1) \cdot Q}{2}}$$

$$= e^{-\frac{1}{M} \frac{Q(Q-1)}{2}}$$

$$Pr[\text{Collison}] \simeq 1 - e^{-\frac{1}{M} \frac{Q(Q-1)}{2}}$$

$$\varepsilon \simeq 1 - e^{-\frac{1}{M} \frac{Q(Q-1)}{2}}$$

$$\Rightarrow e^{-\frac{1}{M} \cdot \frac{Q(Q-1)}{2}} \simeq 1 - \varepsilon$$

$$\Rightarrow -\frac{Q(Q-1)}{2M} \simeq \ln(1-\varepsilon)$$

$$\Rightarrow Q^2 - Q \simeq -2M \ln(1-\varepsilon)$$

$$\Rightarrow Q^2 - Q \simeq 2M \ln\left(\frac{1}{1-\varepsilon}\right)$$

$$\Rightarrow \quad Q^2 \simeq 2M \ln\left(\frac{1}{1-\varepsilon}\right)$$

$$\Rightarrow \quad Q \simeq \sqrt{2M \ln\left(\frac{1}{1-\varepsilon}\right)}$$

$$= \sqrt{2\ln\left(\frac{1}{1-\varepsilon}\right)}\sqrt{M}$$

$$\varepsilon = \frac{1}{2}$$

$$Q \simeq \sqrt{2\ln\left(\frac{1}{1-1/2}\right)}\sqrt{M}$$

$$= \sqrt{2\times \ln 2}\ \sqrt{M}$$

$$\simeq 1.177\sqrt{M}$$

$$\varepsilon = 0.9$$

$$Q \simeq \sqrt{2\times \ln\frac{1}{1-0.9}}\ \sqrt{M}$$

$$\simeq \sqrt{2\times \ln 10}\ \sqrt{M}$$

$$\simeq 2.14\sqrt{M}$$

$$Q = O(\sqrt{M})$$

Complexity of Collison finding

$$= O(\sqrt{M})$$

- $h : X \longrightarrow Y \qquad |Y| \leq 2|X|$

  Preimage $\rightarrow O(|Y|)$

  Collison $\longrightarrow O(\sqrt{|Y|})$

  Second preimage $\rightarrow O(|Y|)$

- $h : \{0,1\}^* \longrightarrow \{0,1\}^m$

  h is secure hash function

  $\rightarrow$ Preimage $\longrightarrow O(2^m)$

  Collison $\longrightarrow O(2^{m/2})$

- Compression function

  $h : \{0,1\}^{m+t} \longrightarrow \{0,1\}^m$

  Preimage $\longrightarrow O(2^m)$

  Collison $\longrightarrow O(2^{m/2})$

Target Construct $H : \{0,1\}^* \longrightarrow \{0,1\}^m$ from h

Security of H will completely depend on security of h.

goal is to compute $H(x)$ using $h(x)$

Given $x \in \{0,1\}^*$

$|x|$ : length of $x$

$|x| \geq m + t + 1$

From $x$ construct $y$ by using a public function. s.t

$$|y| \equiv 0 \pmod t$$

$$y = \begin{cases} x & \text{if } |x| \equiv 0 \pmod t \\ x \| 0^d & \text{if } |x| + d \equiv 0 \pmod t \end{cases}$$

Select $IV \in \{0,1\}^m$ ($IV$ is public)

$$y = y_1 \| y_2 \| \cdots \| y_r$$

s.t. $|y_i| = t$ , $1 \leq i \leq r$

$$H \begin{cases} z_0 = IV \\ z_1 = h(z_0 \| y_1) \\ z_2 = h(z_1 \| y_2) \\ \vdots \\ z_r = h(z_{r-1} \| y_r) \end{cases}$$

$z_r = H(x)$

This is known as iterative hash function

$$x' = z_{r-1} \| y_r$$

$$|x'| = m + t$$

$$IV = z_{r-1}, \quad x^* = y_r, \quad |x^*| \equiv 0 \pmod{t}$$
$$|x^*| = t$$

$$H\left\{ h(z_{r-1} \| y_r) = z_r \right.$$

$$x_1' = z_{r-1}' \| y_r'$$

$$x_2' = z_{r-1}^2 \| y_r^2$$

$$h(x_1') = h(x_2')$$

$$H(x_1') = H(x_2')$$

---

(2) $$M = y_1 \| y_2 \| \cdots \| y_r$$

$$z_r = h(z_{r-1} \| y_r)$$

where $z_i = h(z_{i-1} \| y_i)$ $i = 1, \ldots r-1$

$$z_0 = IV$$

Given $(M, Z_r)$ is it possible to find $(M_2, Z)$ without computing $H$ on $(M_2, Z)$

$\Rightarrow \quad M_2 = M \| y_{r+1}$ $\quad |y_{r+1}| = t$, $H(M) = Z_r$

$h(Z_r \| y_{r+1}) = Z$

length extension Attack

---

## Merkle – Damgard

$h : \{0,1\}^* \rightarrow \{0,1\}$

Compress : $\{0,1\}^{m+t} \rightarrow \{0,1\}^m \quad t \geq 2$

$n = |x|$

$K = \lceil n/(t-1) \rceil$

$d = K \cdot (t-1) - n$

$x = x_1 \| x_2 \| \cdots \| x_K$, $|x_i| = t-1$

for $i = 1$ to $K-1$

$y_i = x_i$

$y_K = x_K \| 0^d$

$y_{K+1} = \text{binary}(d)$

$z_1 = 0^{m+1} \| y_1$

$g_1 = \text{Compress}(z_1)$

for $i = 1$ to $K$

$z_{i+1} = g_i \| 1 \| y_{i+1}$

$g_{i+1} = \text{Compress}(z_{i+1})$

$h(x) = g_{K+1}$

return $(h(x))$

---

(D) SHA – I

MAC

## SHA

Secure Hash Algorithm

i) SHA-160

ii) SHA-256

iii) SHA-512

$$SHA : \{0,1\}^* \longrightarrow \{0,1\}^n$$

## SHA-1 PAD(x)

$$|x| \leq 2^{64} - 1$$

$$d = (447 - |x|) \bmod 512$$

$$l = \text{binary}(|x|)$$

$$y = x \| 1 \| 0^d \| l$$

$|x| + d \equiv 447 \pmod{512}$

$$|y| = |x| + 1 + d + |l|$$

$$\equiv 0 \pmod{512}$$

$447 + 1 + 64 \equiv 0$

- $X \wedge Y$ : bitwise and operation
- $X \vee Y$ : bitwise or operation
- $X \oplus Y$ : bitwise xor operation
- $\neg X$ : bitwise complement
- $X + Y$ : addition mod $2^{32}$

$ROTL^S(x)$ : Circular left shift on x by S position.

$$f_t(B,C,D) = \begin{cases} (B \wedge C) \vee ((\neg B) \wedge D) & 0 \le t \le 19 \\ B \oplus C \oplus D & 20 \le t \le 39 \\ (B \wedge C) \vee (B \wedge D) \vee (C \wedge D) & 40 \le t \le 59 \\ B \oplus C \oplus D & 60 \le t \le 79 \end{cases}$$

## SHA-I (x)

$y = SHA\text{-}I\text{-}PAD(x)$

$y = M_1 \| M_2 \| \cdots \| M_n \quad |M_i| = 512$

$H_0 = 67452301$

$H_1 = EFCDAB89$

$H_2 = 98BADCFE$

$H_3 = 10325476$

$H_4 = C3D2E1F0$

$$K_t = \begin{cases} 5A827999 & 0 \le t \le 19 \\ 6ED9EBA1 & 20 \le t \le 39 \\ 8F1BBCDC & 40 \le t \le 59 \\ CA62C1D6 & 60 \le t \le 79 \end{cases}$$

for $i = 1$ to $n$

$M_i = w_0 \| w_1 \| w_2 \| \cdots \| w_{15}$ ; $|w_i| = 32$

for $t = 16$ to 79

$W_t = ROTL^1 (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16})$

$A = H_0$

$B = H_1$

$C = H_2$

$D = H_3$

$E = H_4$

for $t = 0$ to 79

$temp = ROTL^5(A) + f_t(B, C, D) + E + W_t + K_t$

$E = D$

$D = C$

$C = ROTL^{30}(B)$

$B = A$

$A = temp$

$H_0 = H_0 + A$

$H_1 = H_1 + B$

$$H_2 = H_2 + C$$

$$H_3 = H_3 + D$$

$$H_4 = H_4 + E$$

Return $( H_0 \| H_1 \| H_2 \| H_3 \| H_4 )$

---

☑ **MAC**

Message authentication Code

| Alice | | Bob |
|---|---|---|
| K | | K |
| $C = Enc(M, K)$ | $\xrightarrow{C}$ | $\tilde{C}$ |
| $MAC = Hash(M, K)$ | $\xrightarrow{MAC}$ | $\tilde{MAC}$ |

$$Dec(\tilde{C}, K) = \tilde{M}$$

$$Hash(\tilde{M}, K) = MAC_1$$

if $MAC_1 = \tilde{MAC}$

accept $\tilde{M}$

as $\tilde{M} = M$

## HMAC

ipad = 36 36 ... 36 → 512 bits

opad = 5C 5C ... 5C → 512 bits

K → Secret key

$$HMAC_K(x) = SHA\text{-}1\Big((K \oplus opad) \,||\, SHA\text{-}1\big((K \oplus ipad) \,||\, x\big)\Big)$$

## CBC-MAC (x, K)

$x = x_1 || \ldots || x_n$

IV = 00 ... 0

$y_0 = IV$

for $i = 1$ to $n$

$y_i = Enc\big((y_{i-1} \oplus x_i), K\big)$

return $(y_n)$

LECTURES BY SHREEDARSHAN

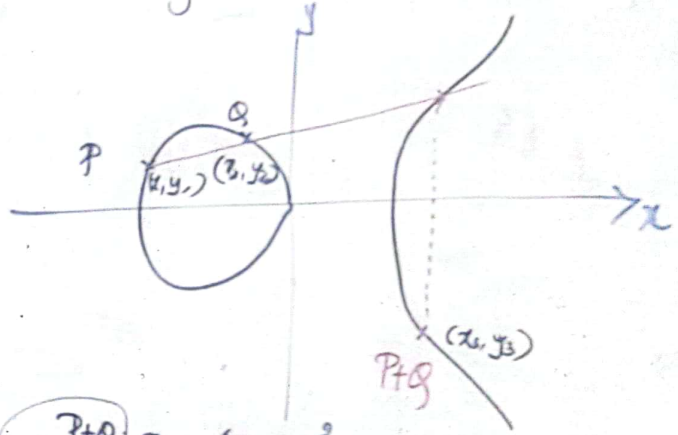
# Elliptic Curve Cryptography P+Q, 2P $y^2 = x^3 - x$

$y^2 = x^3 + ax + b$

\# $E_{23}(1,1)$ $y^2 = x^3 + x + 1 \pmod{23}$ $(0 \cdots 22)$ 36

i) $P = (13,7)$; $-P = (x, -y) = (13,-7) = (13,16)$

ii) $R = P + Q$ $P = (3,10)$ $(x_1, y_1)$ $Q = (9,7)$




To find 2P $x_3 = \left(\frac{3x9+1}{2x10}\right)^2 - 6 = \left(\frac{28}{20}\right)^2 + 17$

$\left(\frac{5}{2/4}\right)^2 + 17 = \left(\frac{1}{4}\right)^2 + 17 = (1.4^{-1})^2 + 17$

$6^2 + 17 = \underline{36+17} = \underline{7}$ (53)

$y_3 = -10 + \left(\frac{3x9+1}{2x10}\right)(3-7) = 13 + \left(\frac{28}{20}\right) \times -4$

$= 13 + \left(\frac{1}{4}\right) \times -4 = 13$

P+Q; $x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$

$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3)$

2P P=Q

$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$

$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3)$

OPPO Reno2 F

LECTURES BY SHREEDARSHAN

# Elliptic Curve Cryptography P+Q, 2P $y^2 = x^3 - x$

$y^2 = x^3 + ax + b$

\# $E_{23}(1,1)$ $y^2 = x^3 + x + 1 \pmod{23}$ $(0 \cdots 22)$ 36

$= (13,7)$; $-P = (x, -y) = (13,-7) = (13,16)$

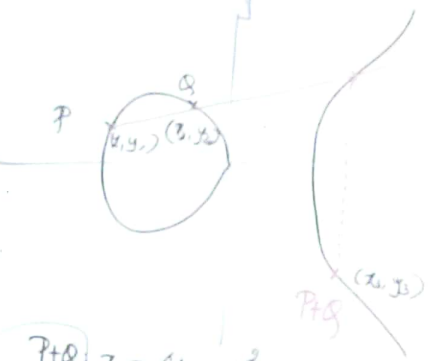
$R = P + Q$ $P = (3,10)$ $(x_1, y_1)$ $Q = (9,7)$

To find 2P $x_3 = \left(\frac{3.9+1}{2.10}\right)^2 - 6 = \left(\frac{28}{20}\right)^2 + 17$

$\left(\frac{5}{2}\right)^2 + 17 = \left(\frac{1}{4}\right)^2 + 17 = (1.4^{-1})^2 + 17$

$6^2 + 17 = \underbrace{36+17}_{53} = 7$

$y_3 = -10 + \left(\frac{3.9+1}{2.10}\right)(3-7) = 13 + (28) \cdot -4$




P+Q; $x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$

$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3)$

2P P=Q

$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$

$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3)$

OPPO Reno2 F

ideapad GAMING

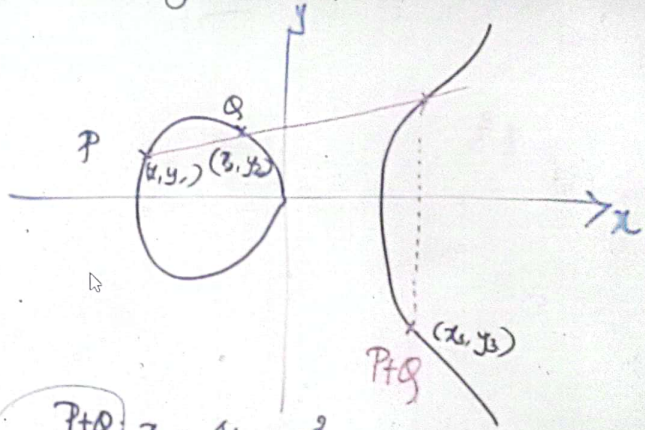
ic Curve Cryptography |Find points P+Q and 2P |ECC in Cryptography & Security

ES BY
RSHAN

# Elliptic Curve Cryptography P+Q, 2P

$y^2 = x^3 + ax + b$

$y^2 = x^3 - x$




# $y^2 = x^3 - 36x$, $P = (-3, 9)$, $Q = (-2, 8)$ ; $a = -36$

$(x_1, y_1)$ $(x_2, y_2)$

P+Q, & 2P

P+Q = (6, 0)

$x_3 = \left(\frac{8-9}{-2+3}\right)^2 - (-3) - (-2) = 1^2 + 3 + 2 = 6$

$y_3 = -9 + \left(\frac{8-9}{-2+3}\right)(-3-6) = -9 - 1(-9) = 0$

2P $x_3 = \left(\frac{3(-3)^2 + (-36)}{2 \times 9}\right)^2 - 2(-3) = \left(\frac{27-36}{18}\right)^2 + 6$

$x_3 = 1/4 + 6 = 25/4$

$y_3 = -9 + \left(\frac{3 \cdot 9 - 36}{18}\right)(-3 - 25/4) = -35/8$

$2P = (25/4, -35/8)$

P+Q; $x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$

$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3)$

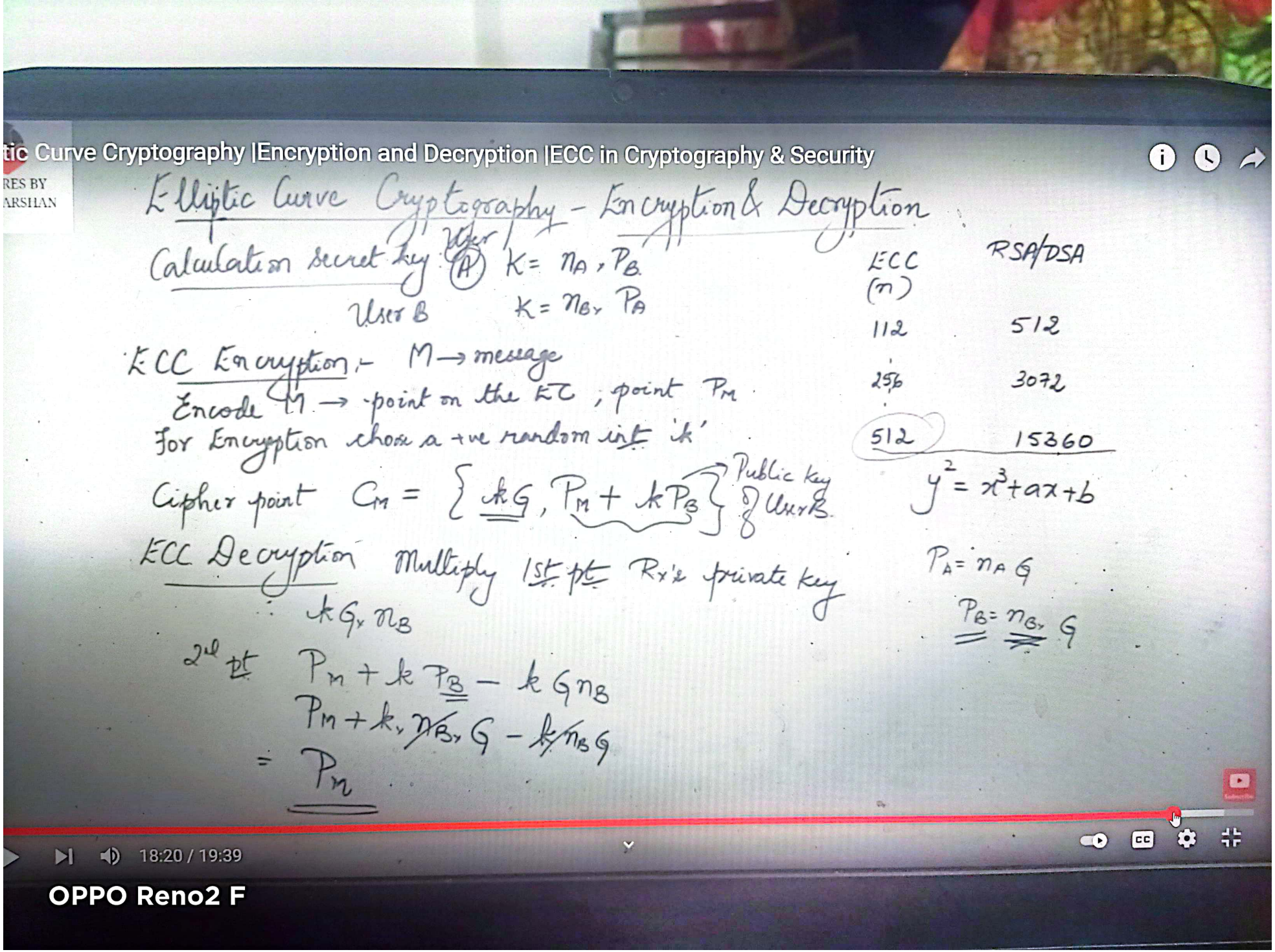
2P P=Q

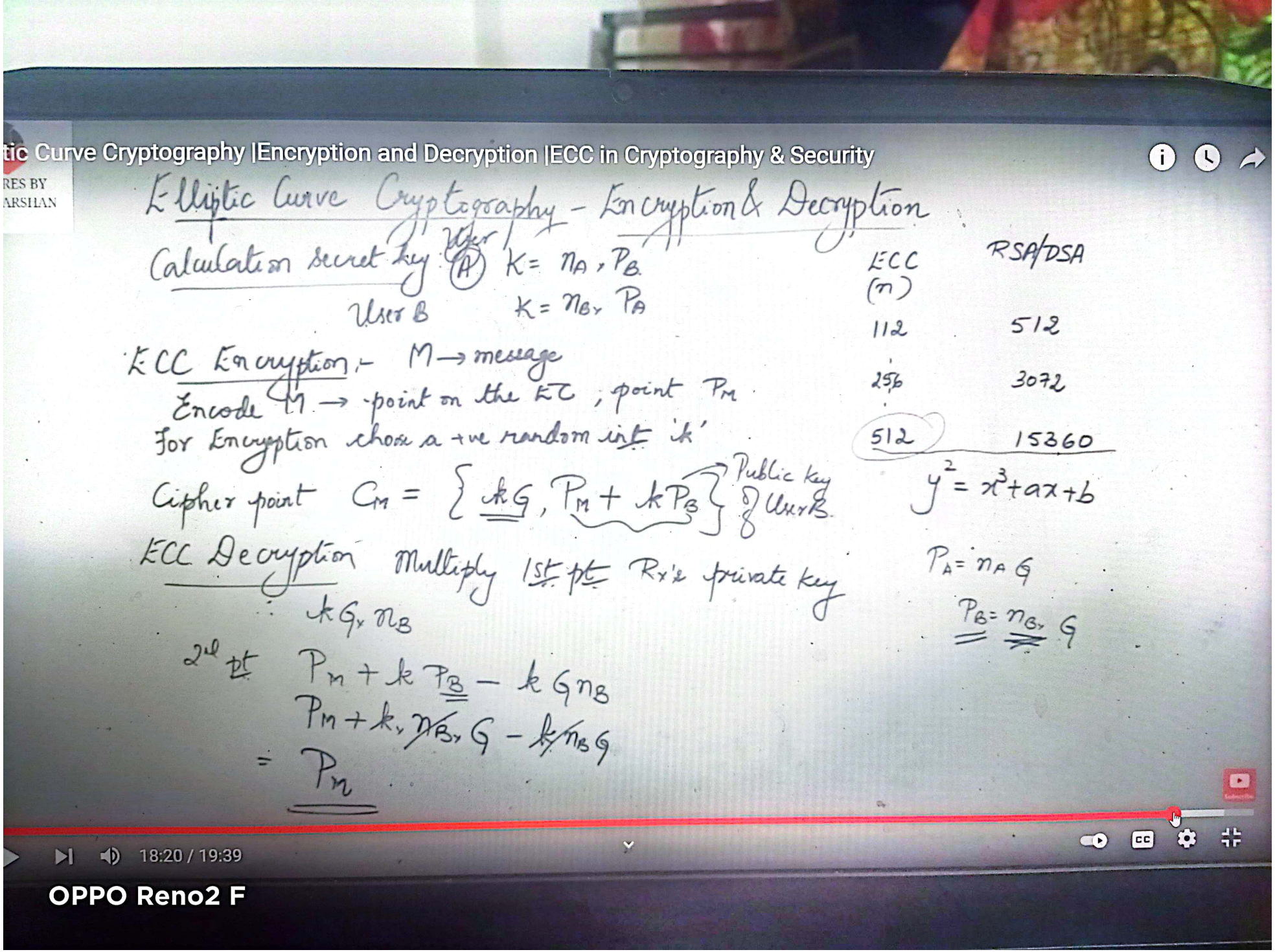
$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$

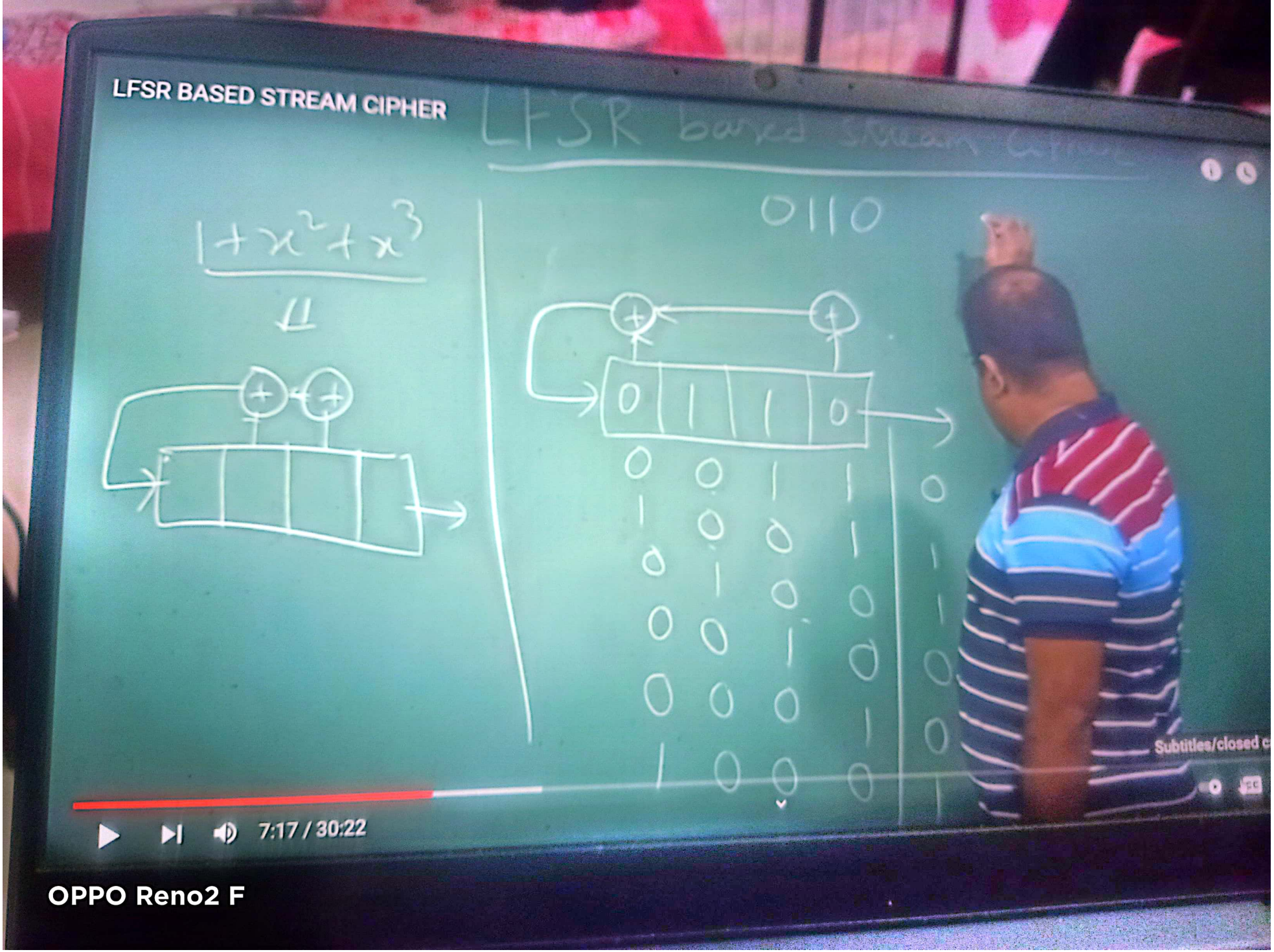
$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3)$

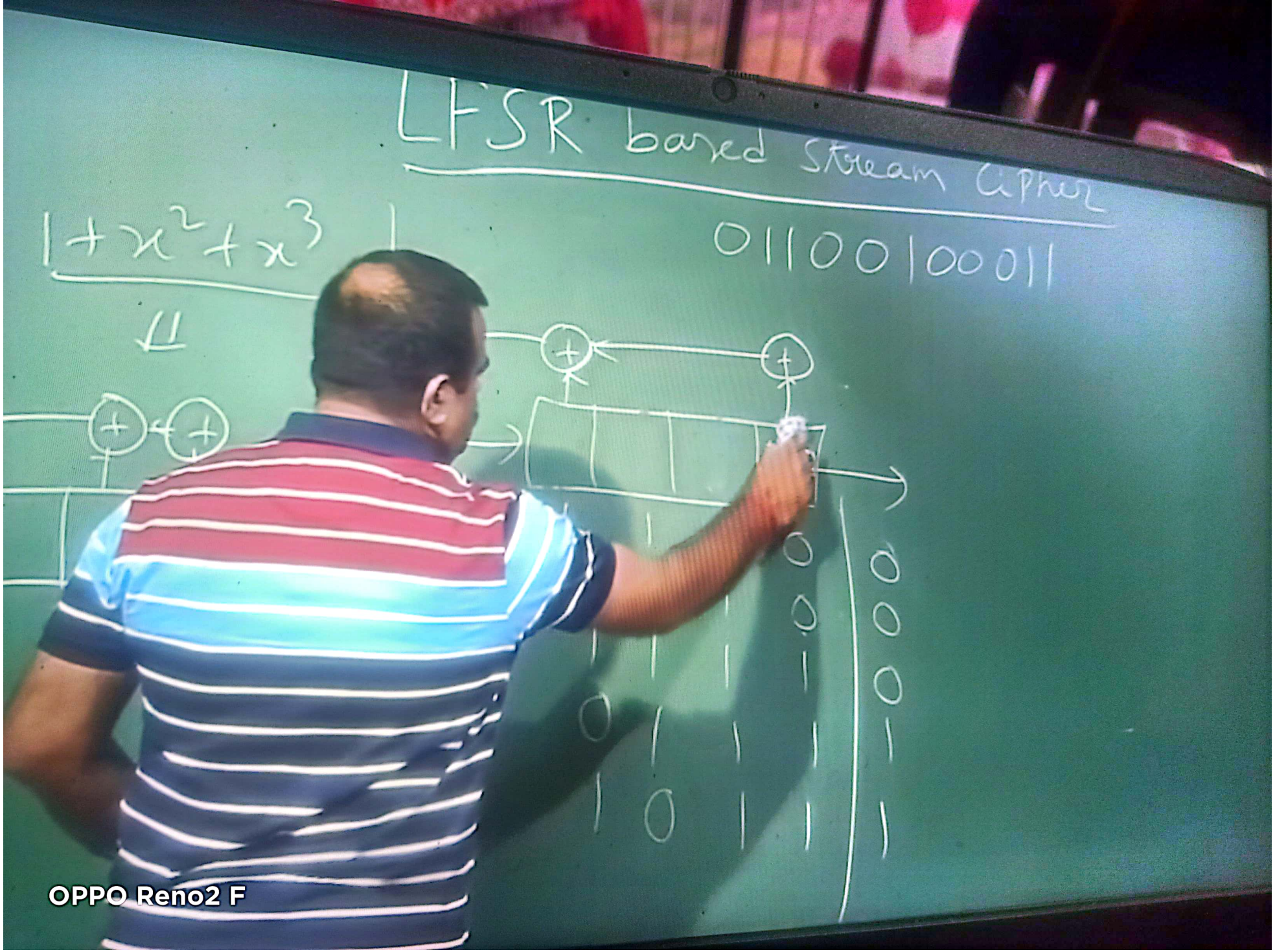
8:57 / 17:44

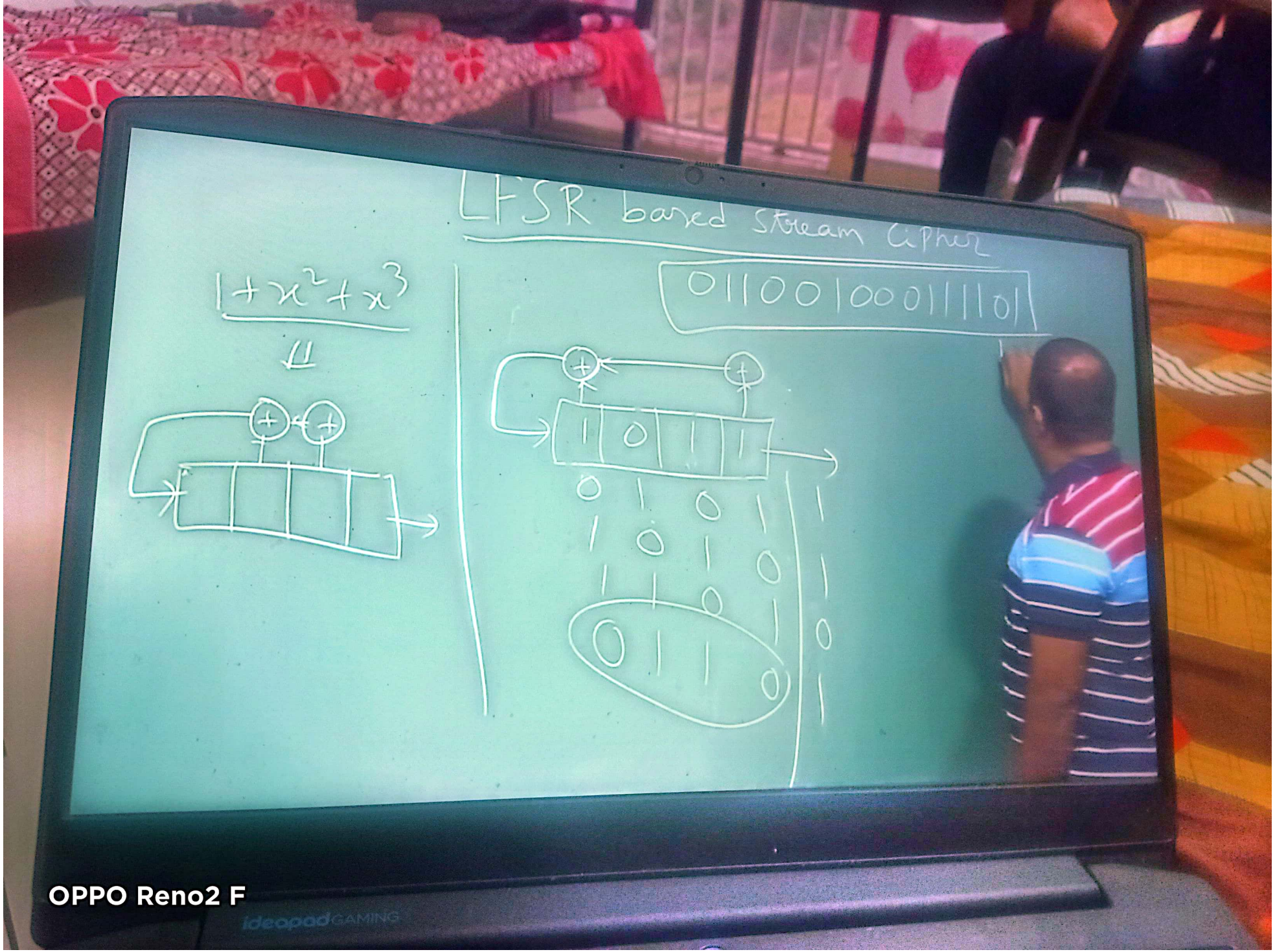
OPPO Reno2 F

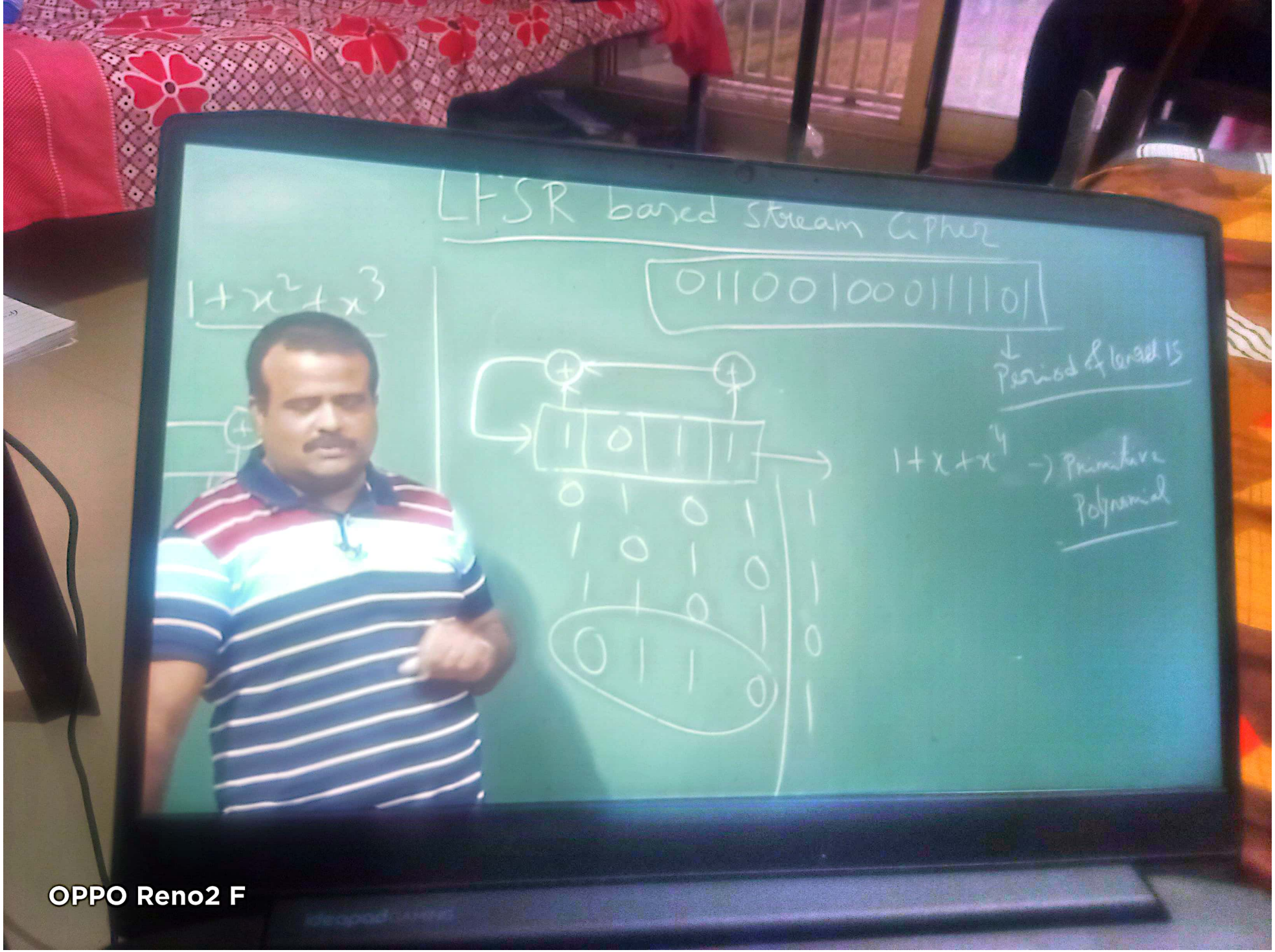


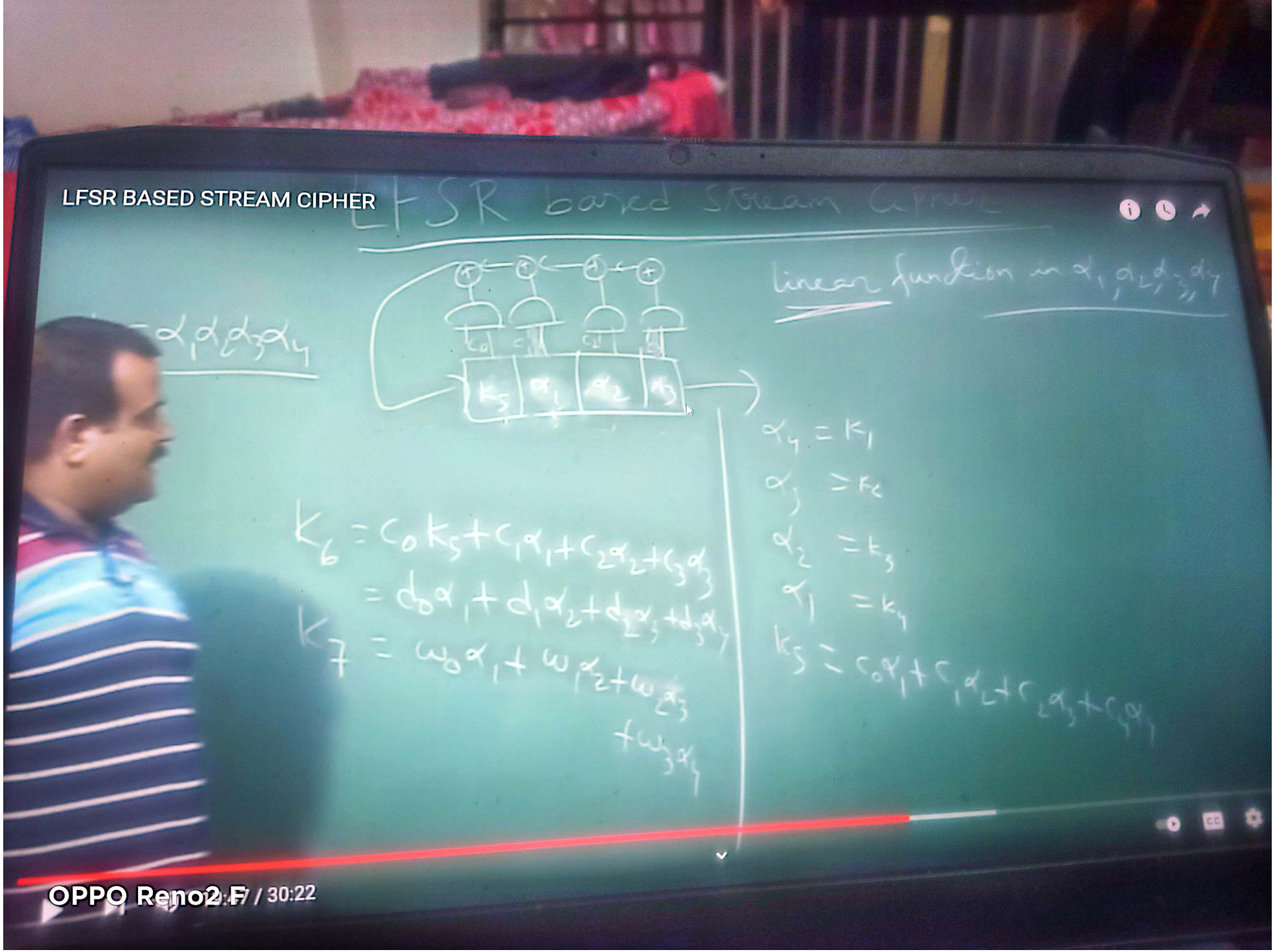


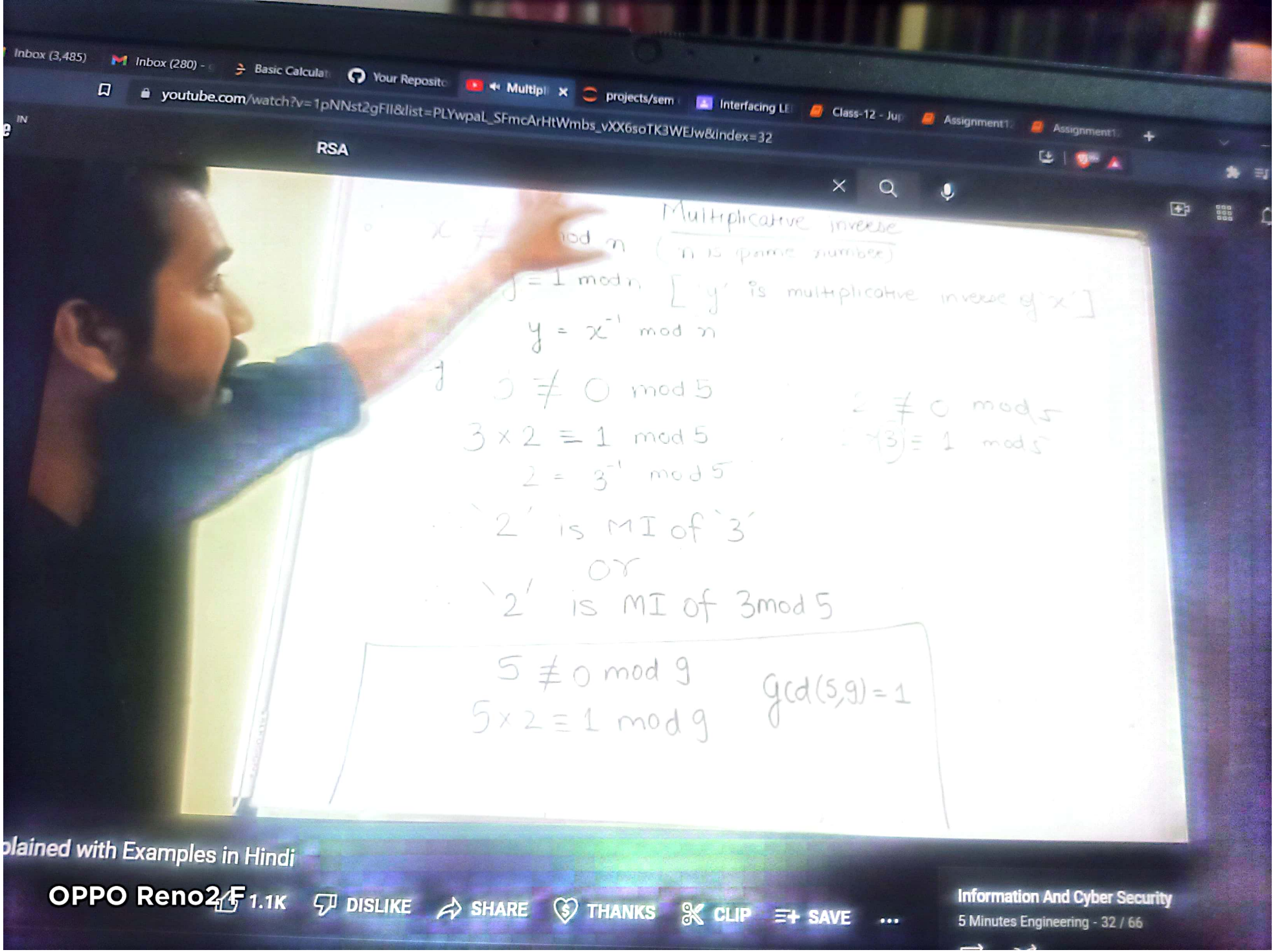


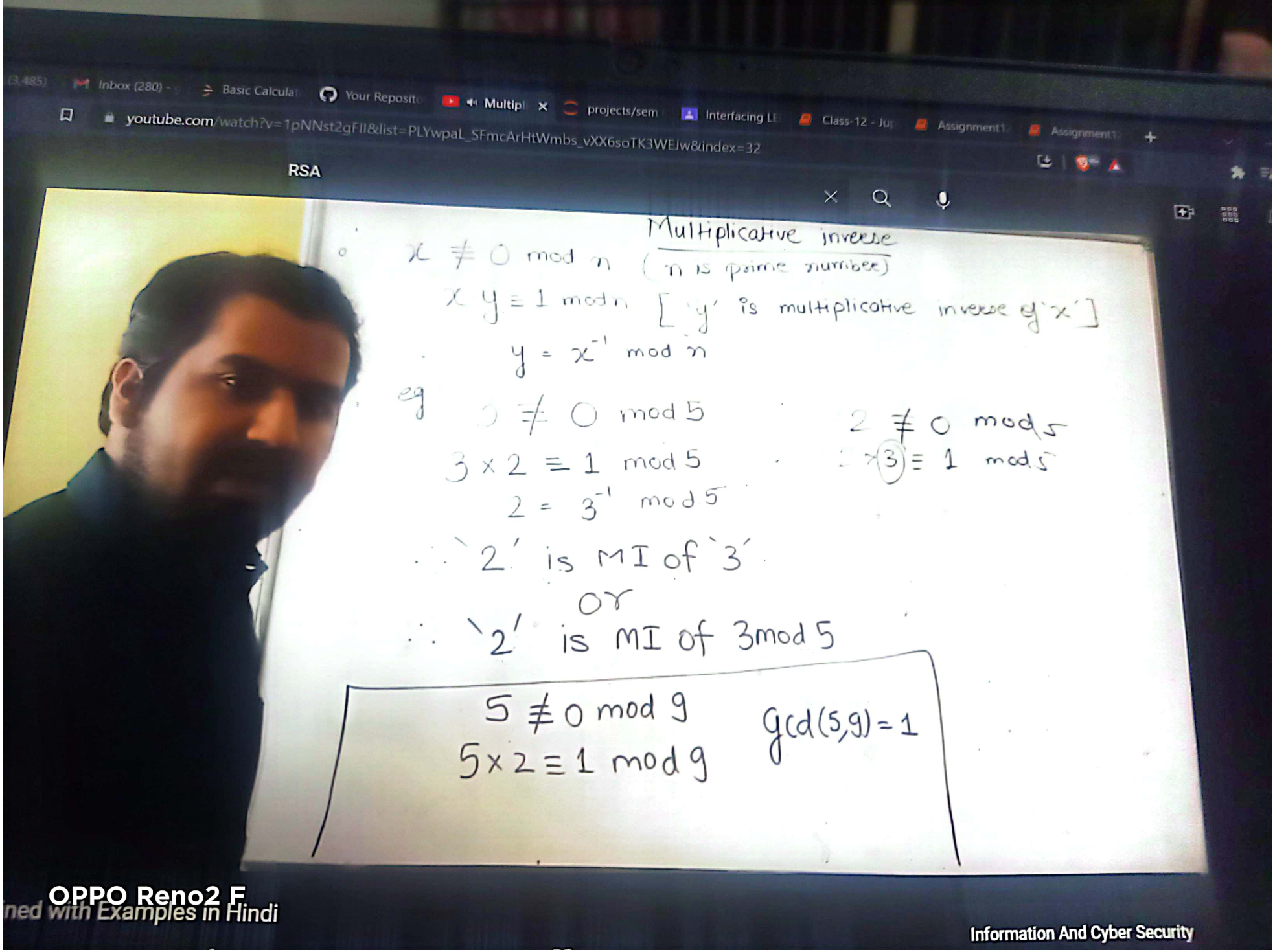


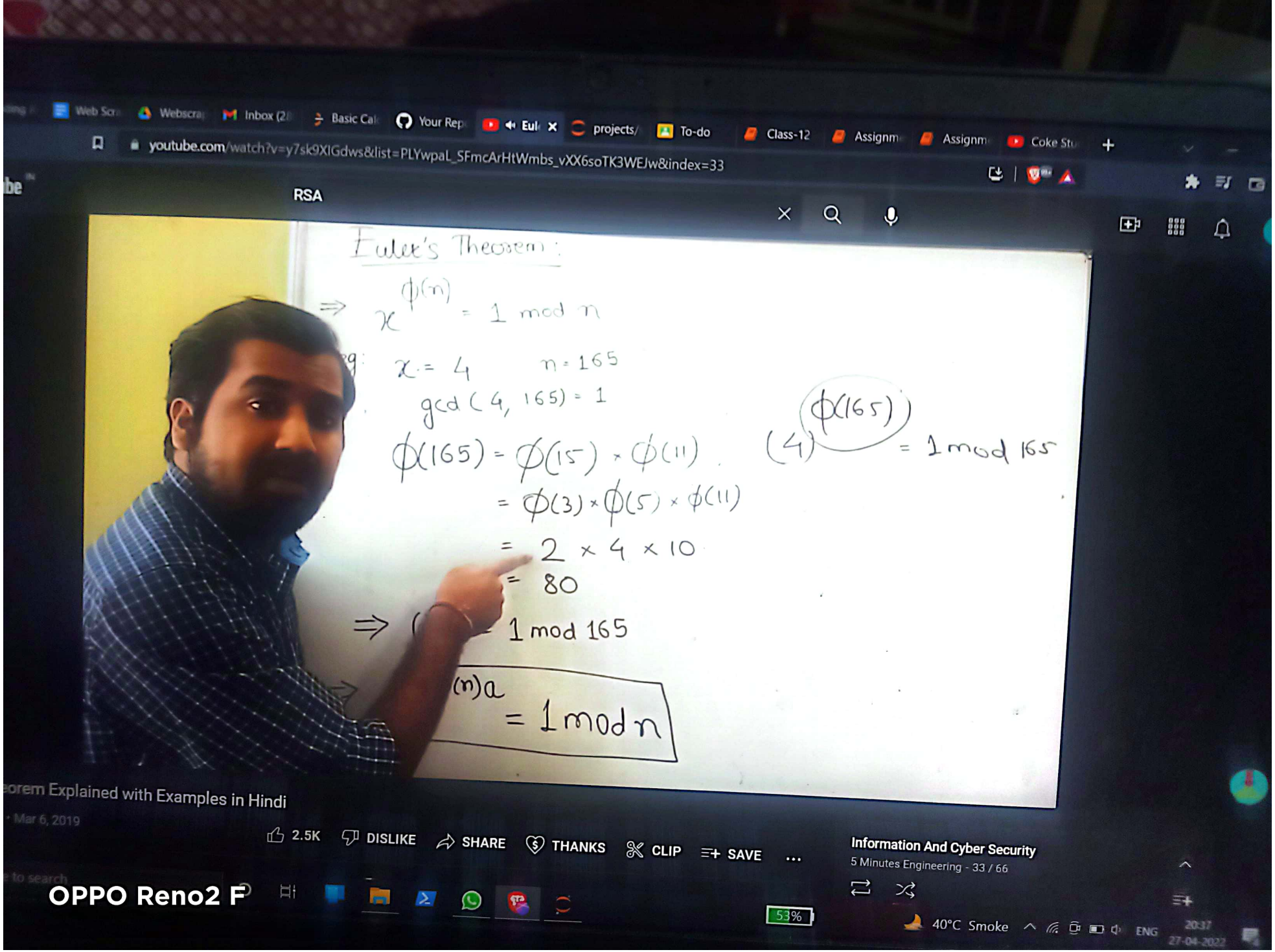


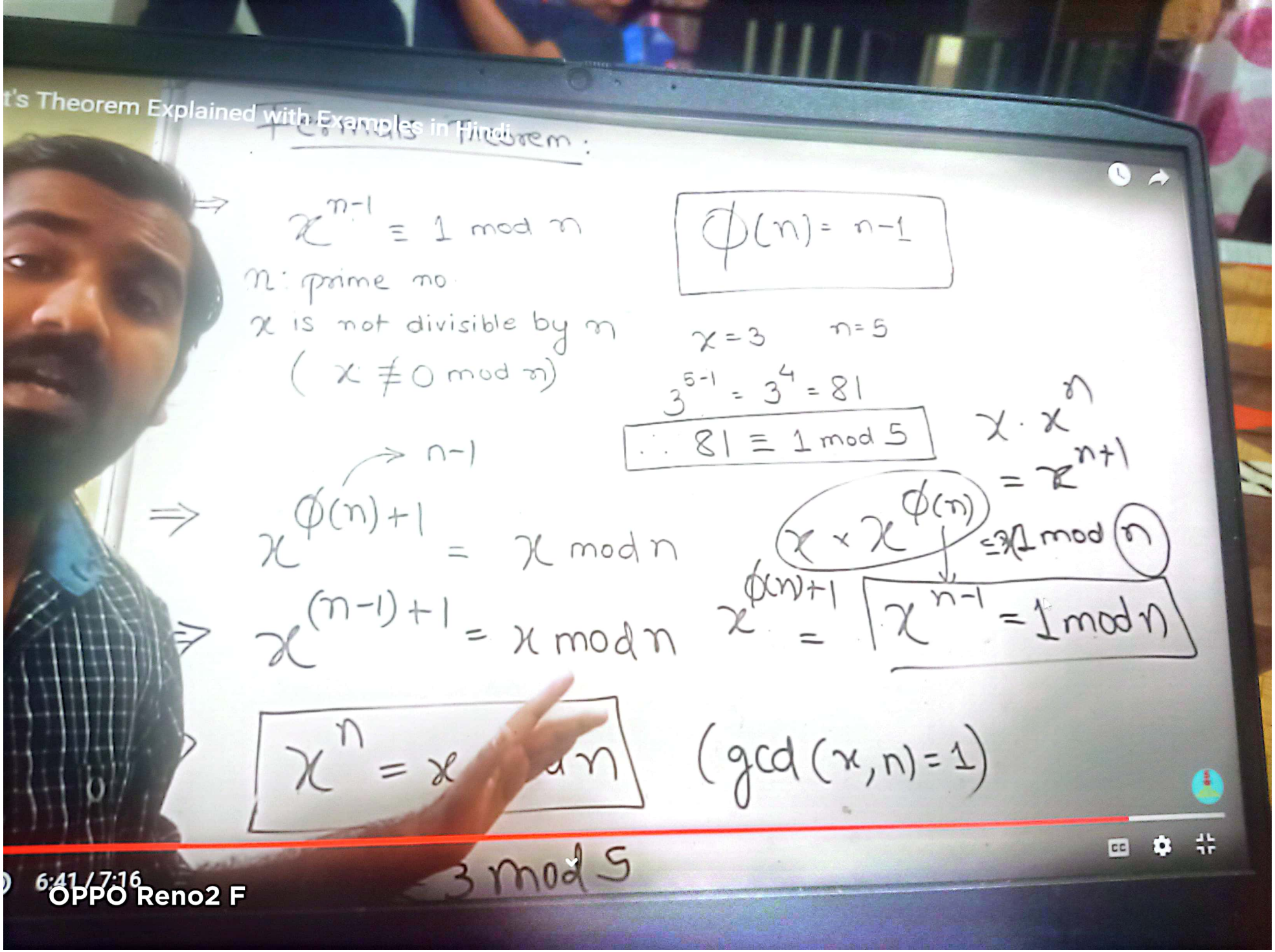


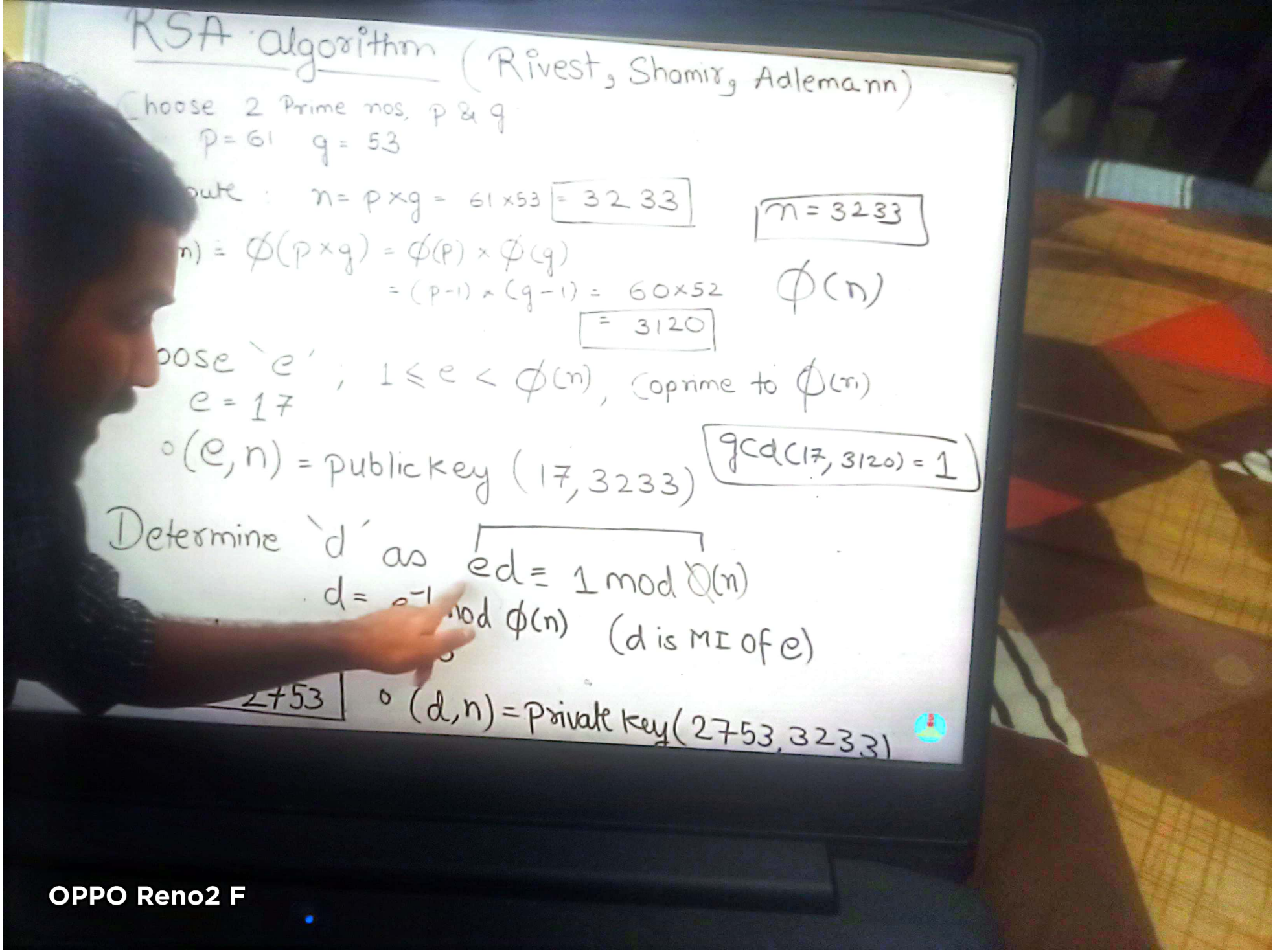


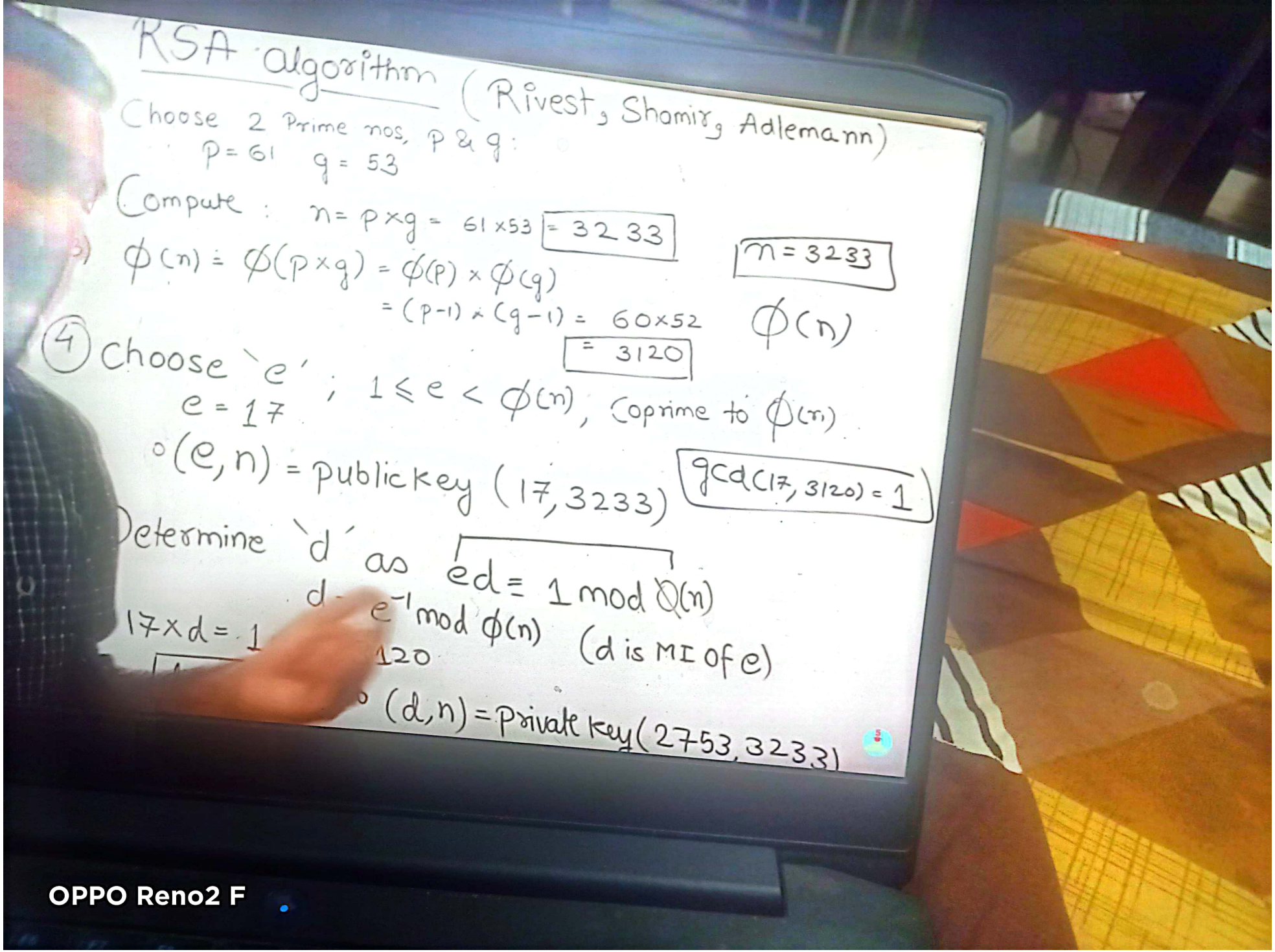


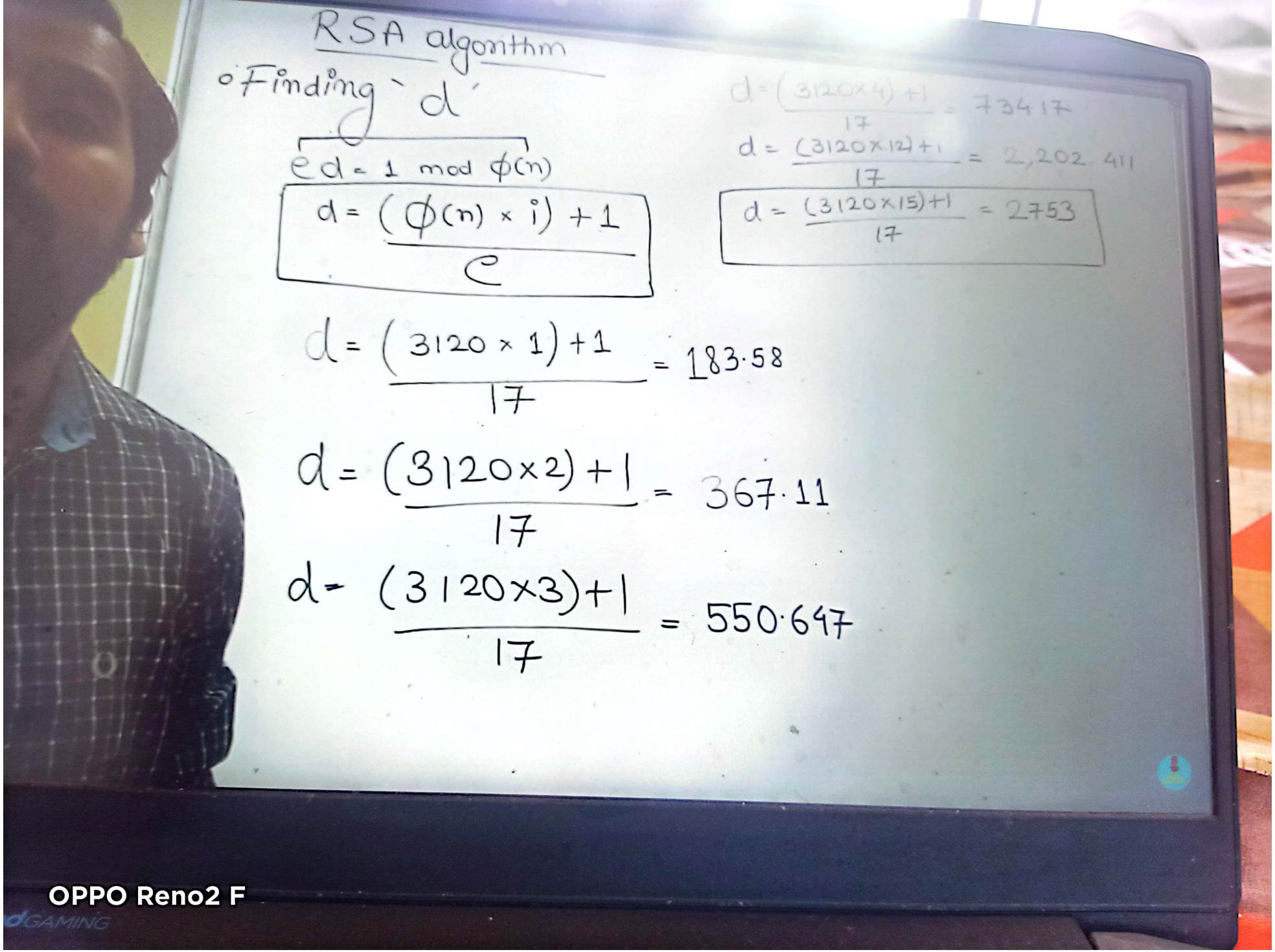


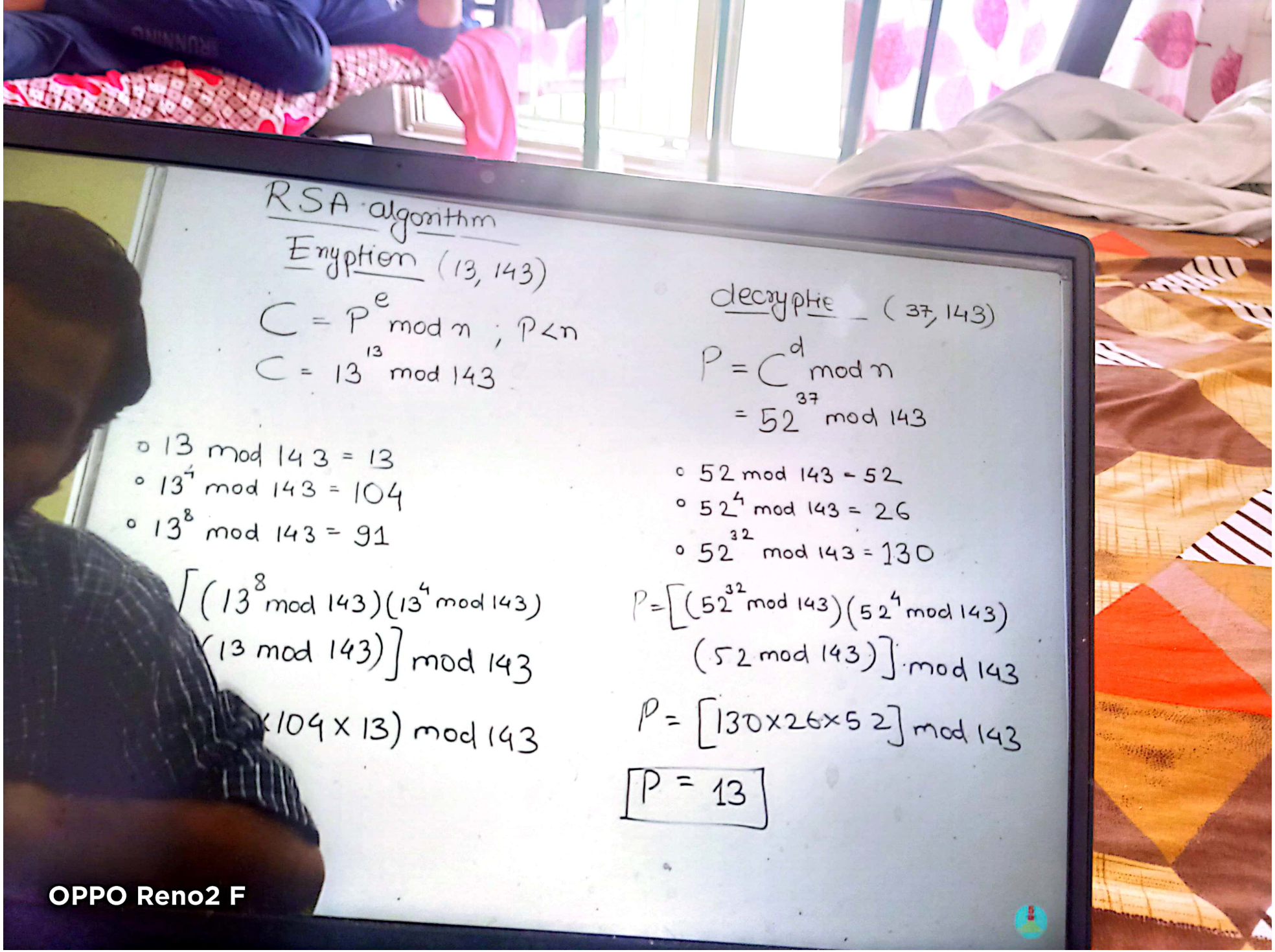


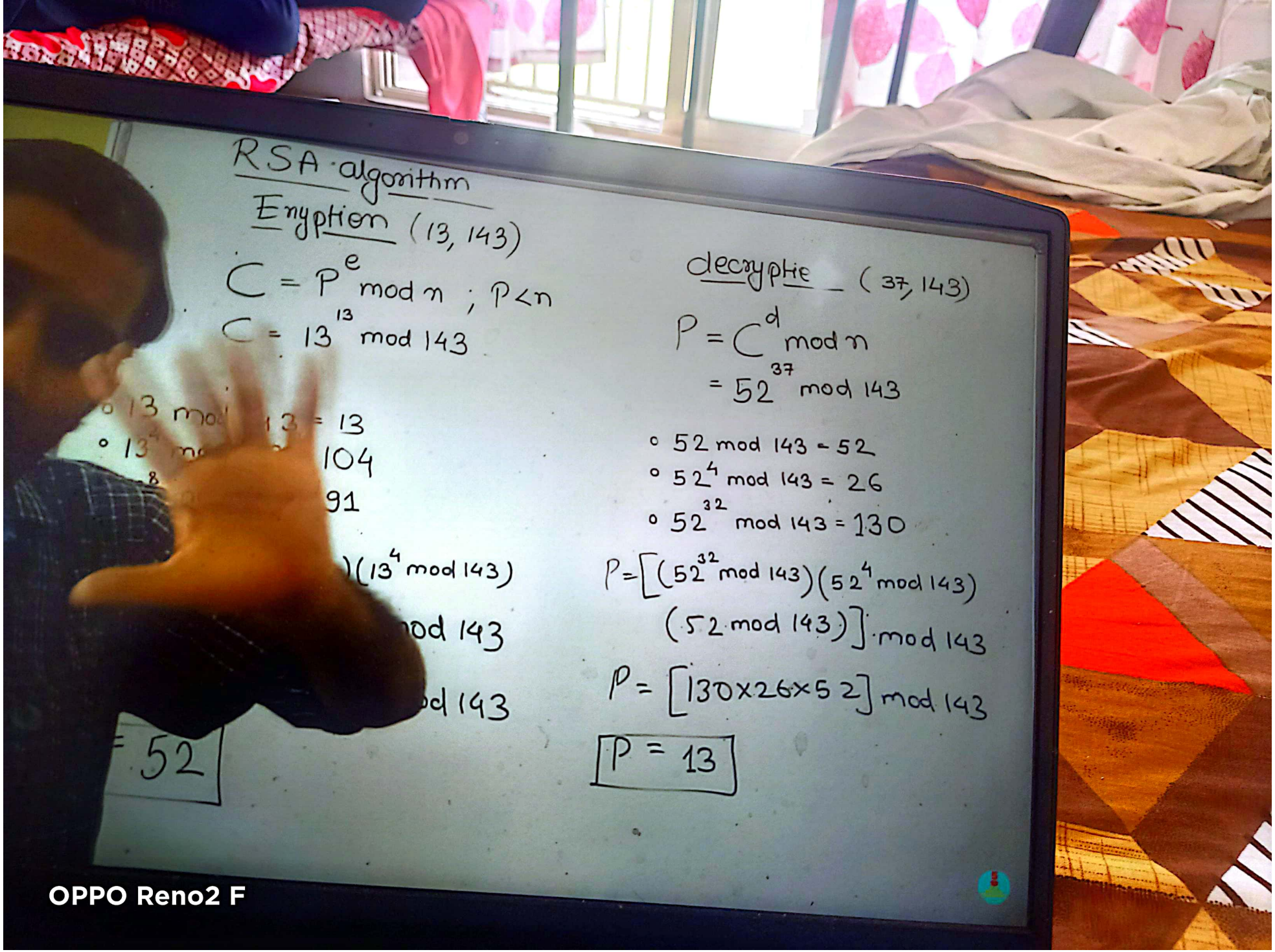


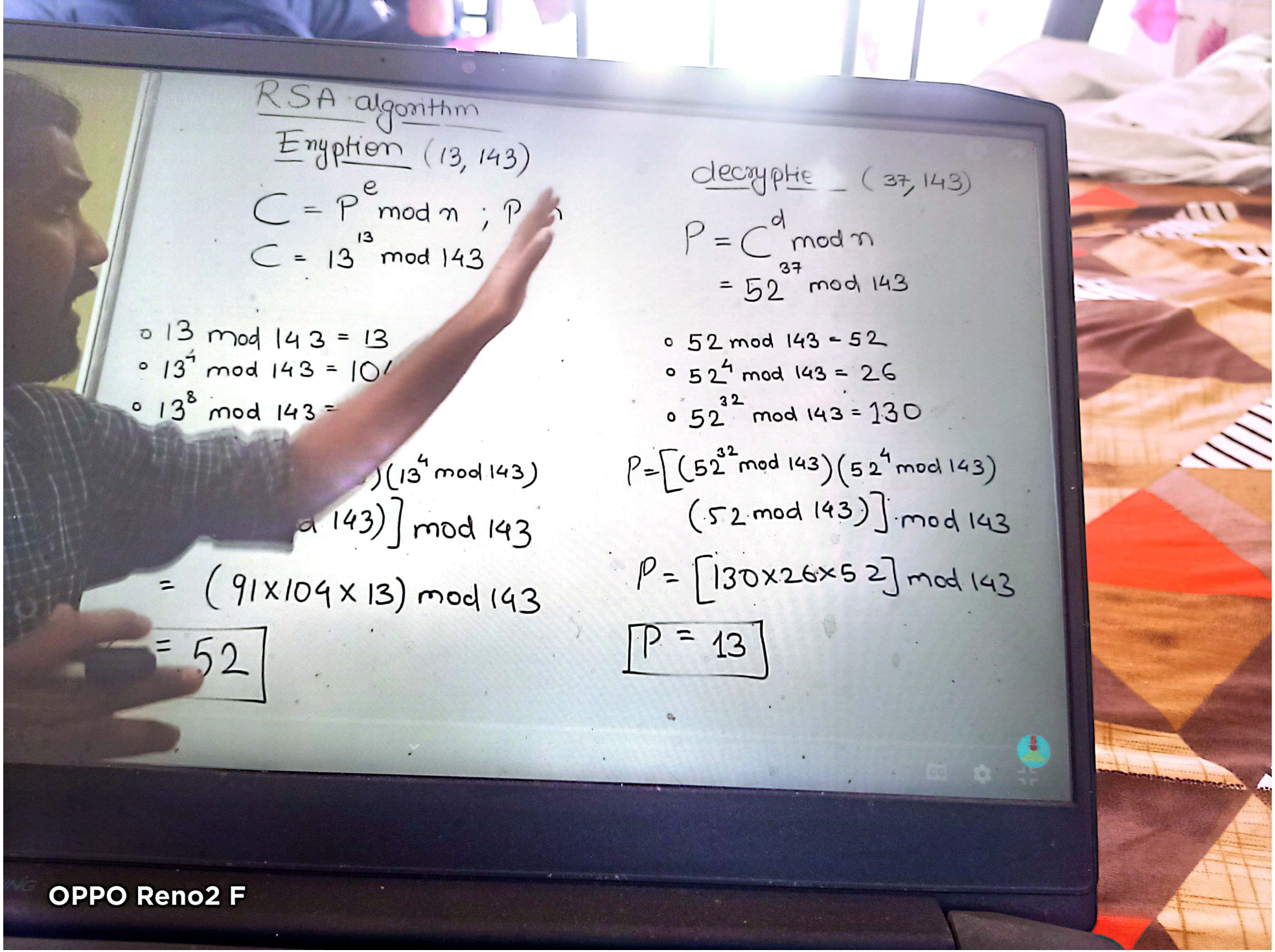


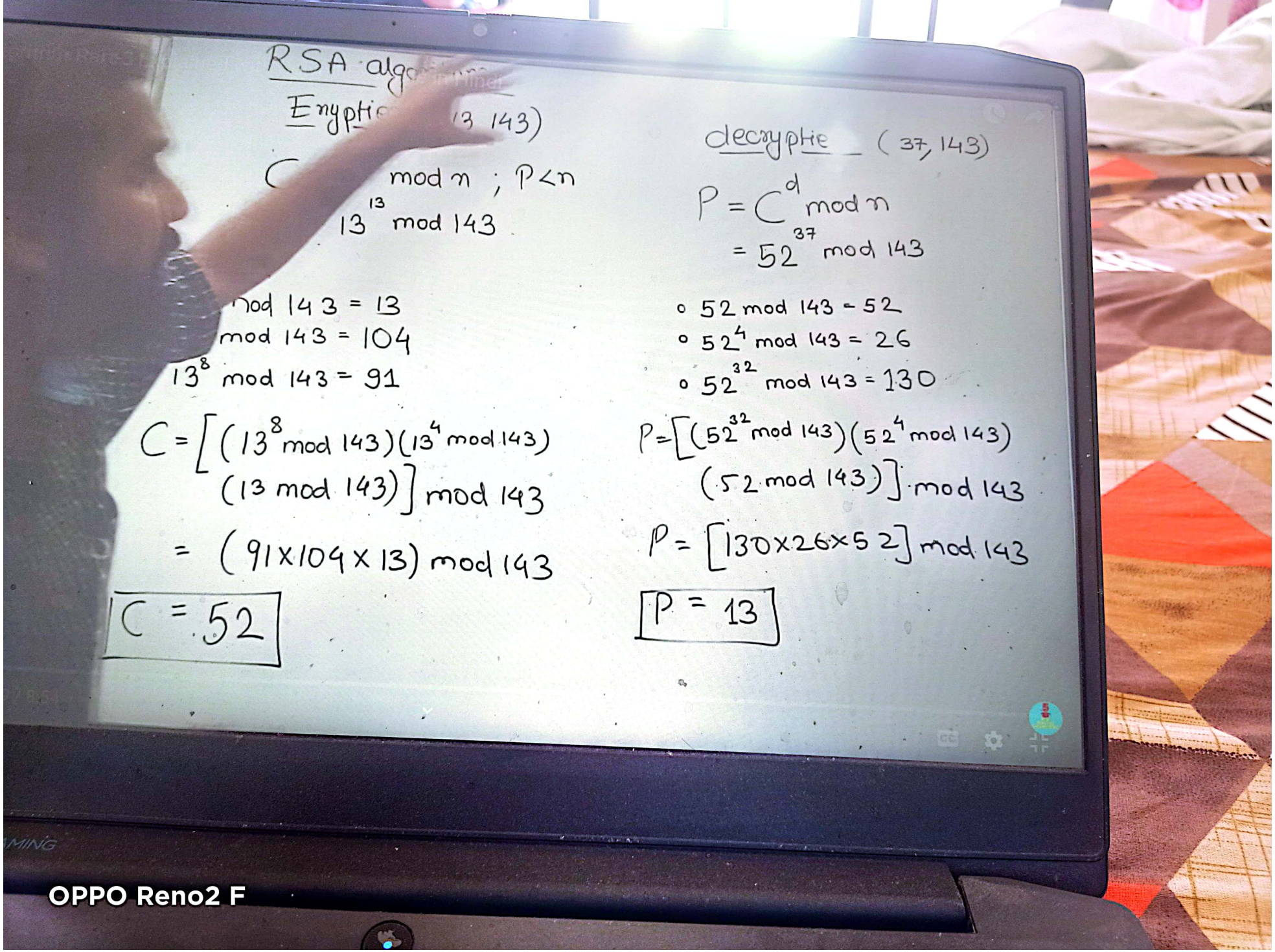


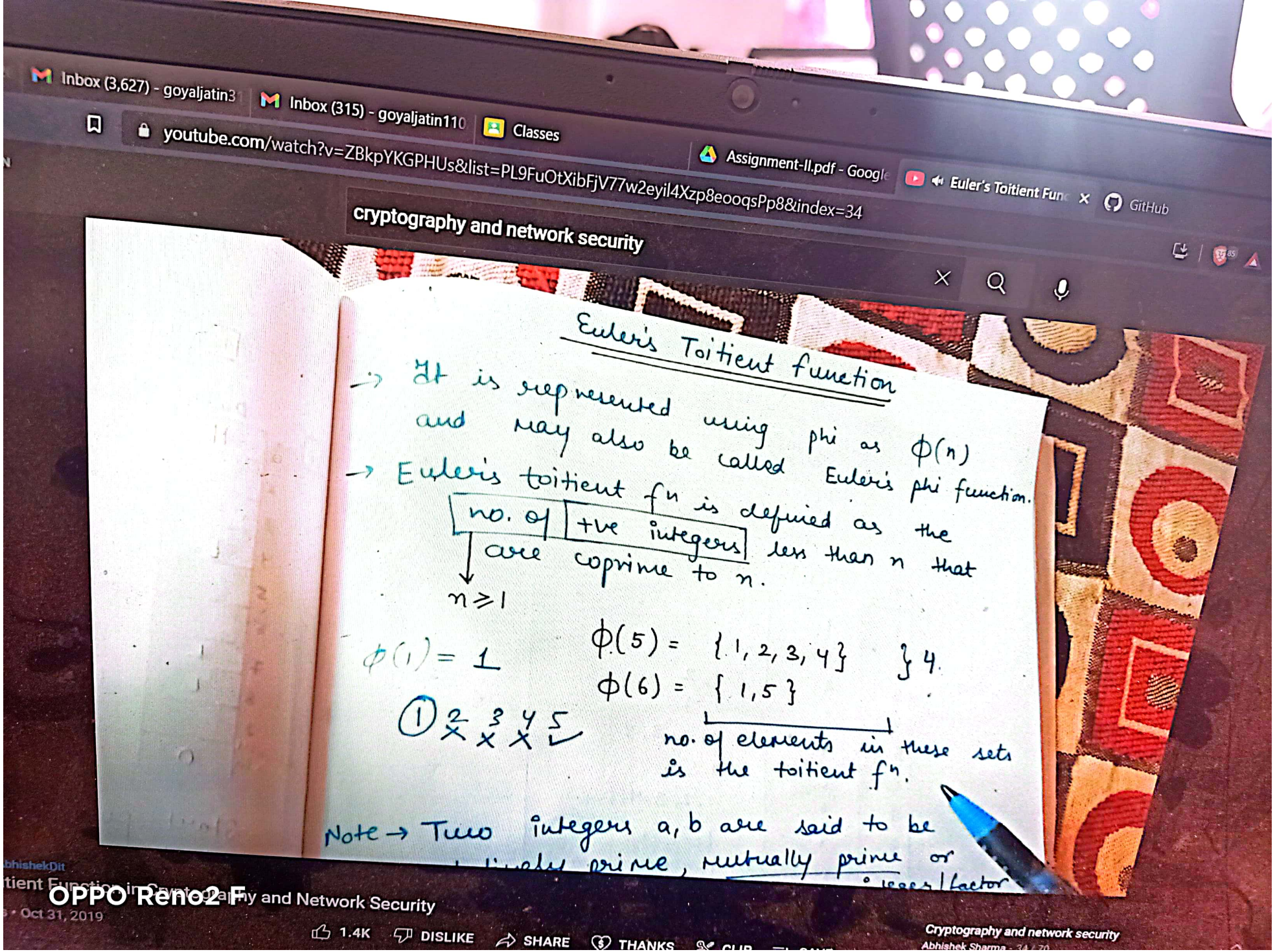


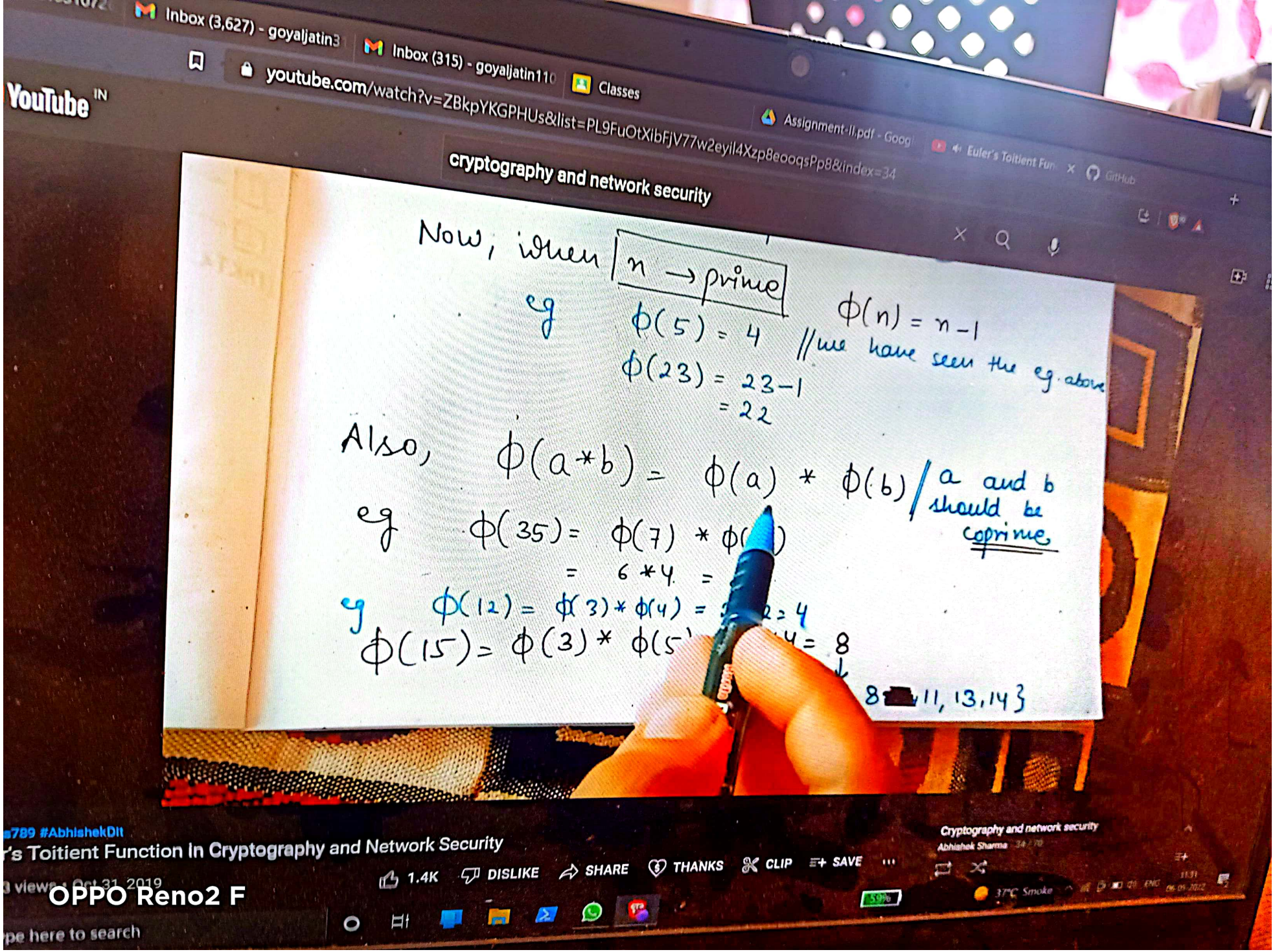


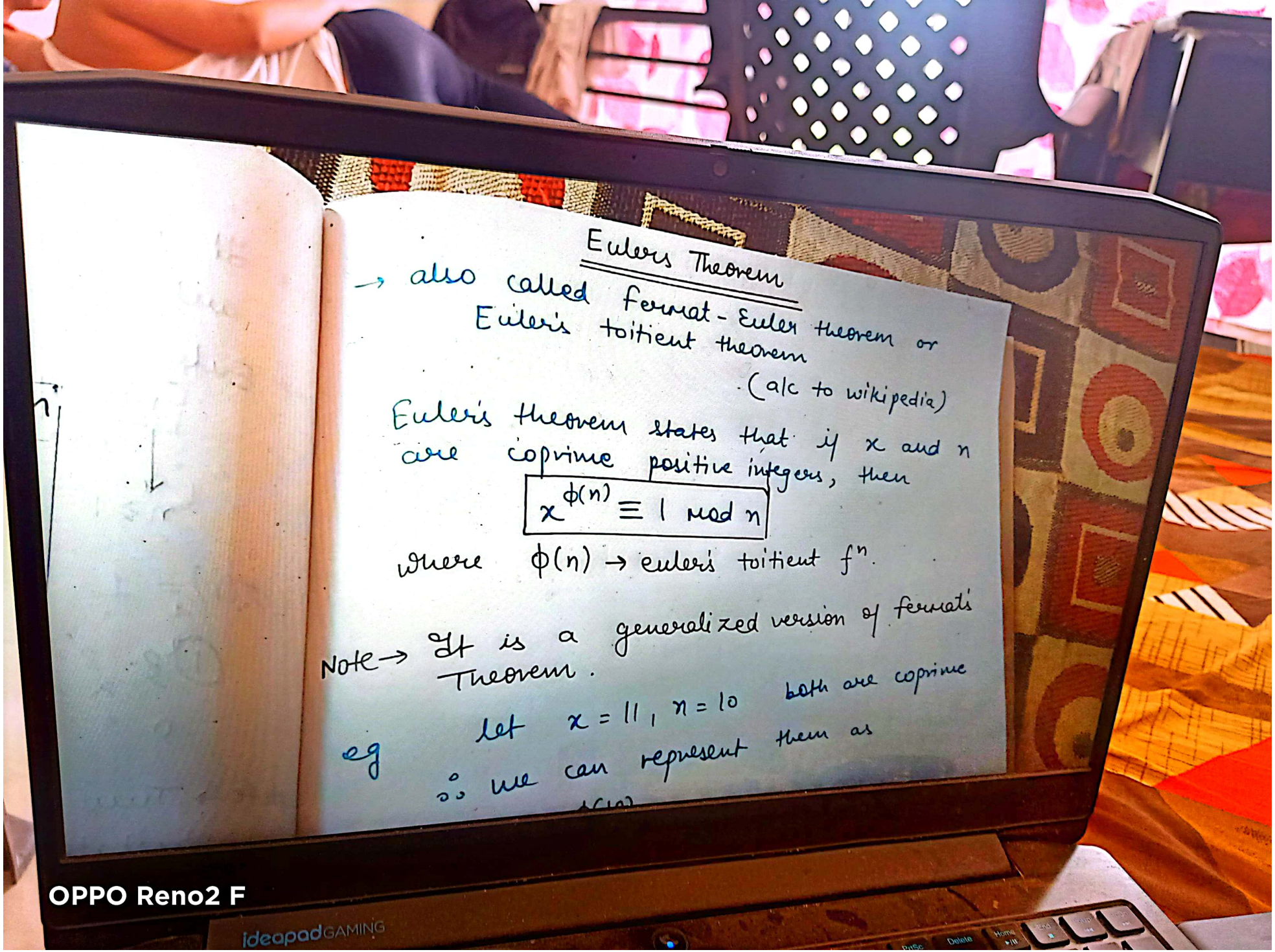


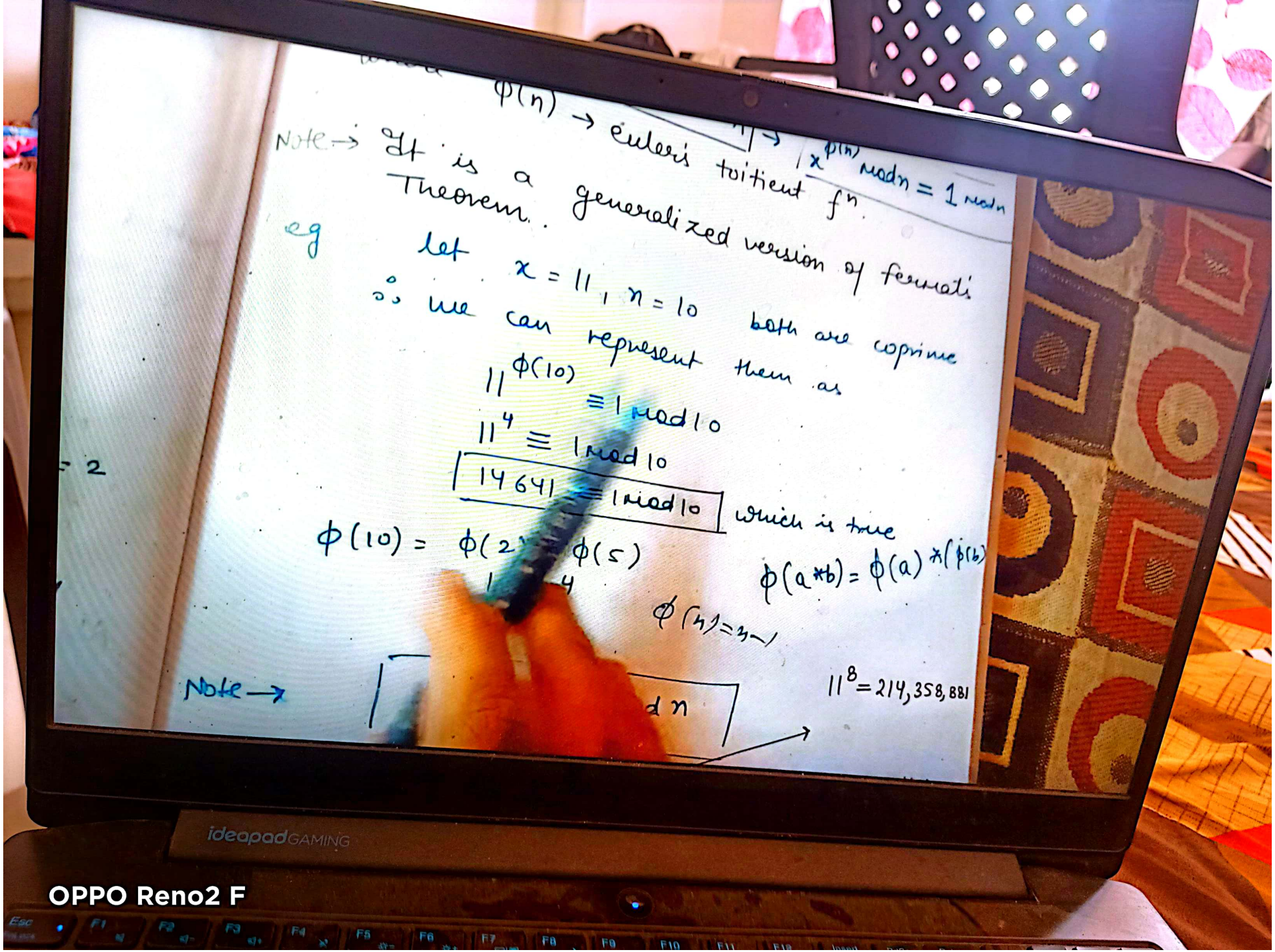












# $4^{99}$ Mod 35

$x = 4, \quad n = 35$

by eulers theorem,

$4^{\phi(35)} = 1 \bmod 35$

$4^{24} \equiv 1 \bmod 35$ —(1)

eulers theorem

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

$x, n \rightarrow$ coprime +ve integers

$\phi(n) = n-1$

$\phi(35) = \phi(7) \cdot \phi(5)$

$= 6 \times 4$

$\phi(35) = 24$

$4^{24 \times 4 + 3}$

$99 = 24(4) + 3$

$4^3$

$\equiv 1 \bmod n$

$\equiv 1 \bmod n$

$35 = 4^{24 \times 4 + 3} \bmod 35$

$= (4^{24})^4 \cdot 4^3 \bmod 35$

$= (4^{24})^4 \bmod 35 \cdot 4^3 \bmod 35$

$\bmod n \equiv (a \bmod n)(b \bmod n)$

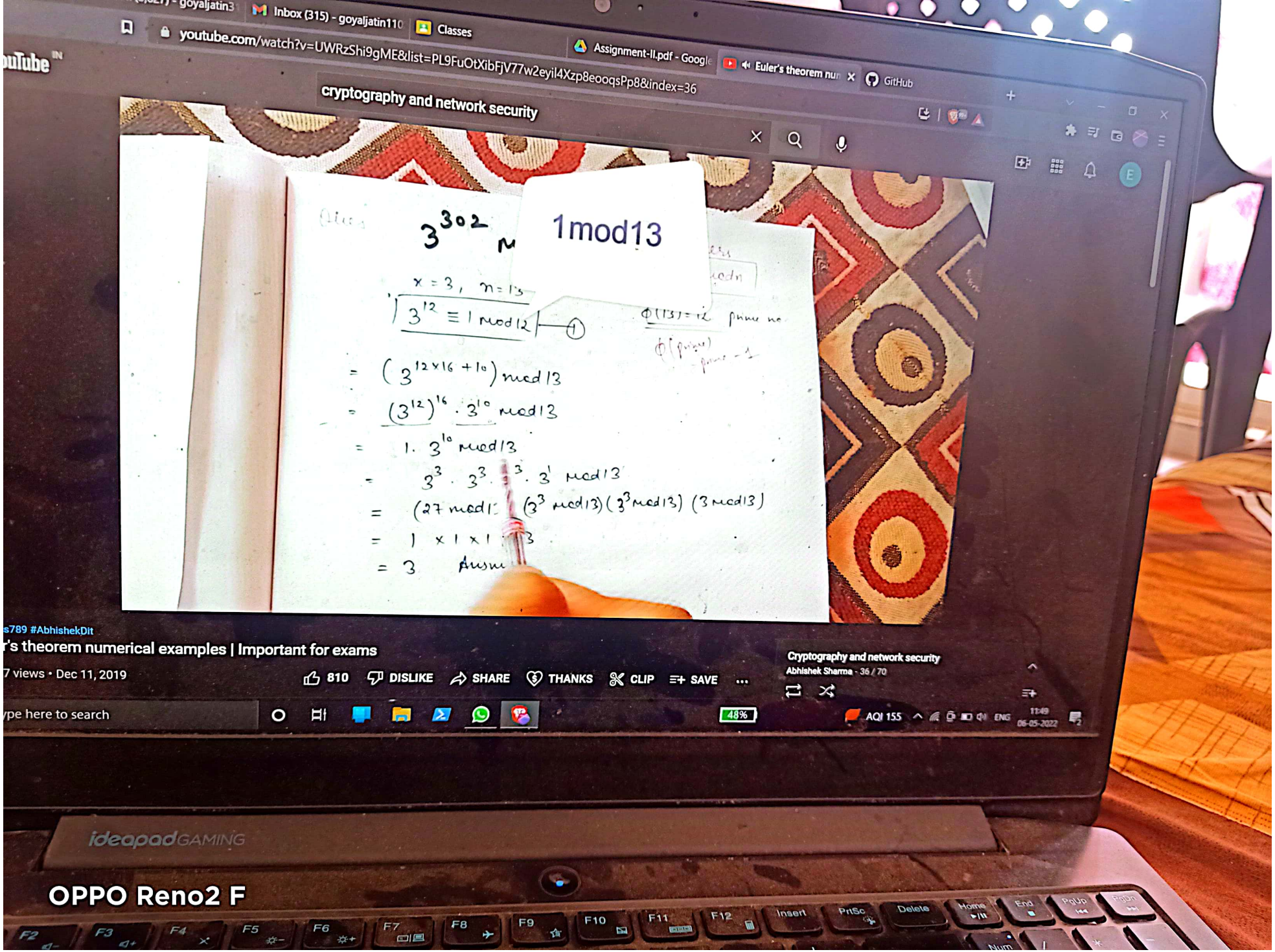
$= 1 \times 4^3 \bmod 35$

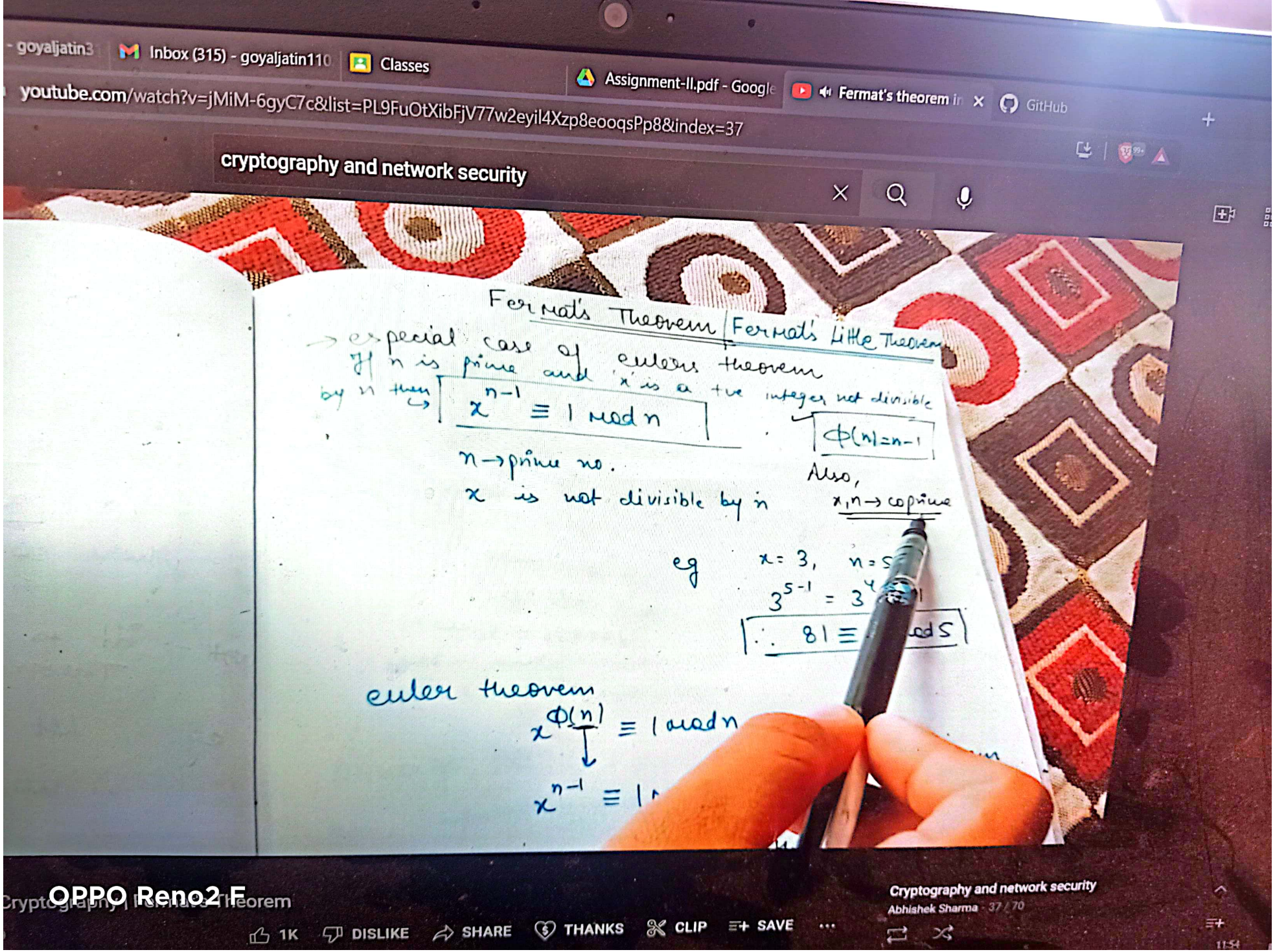
$= 64 \bmod 35$

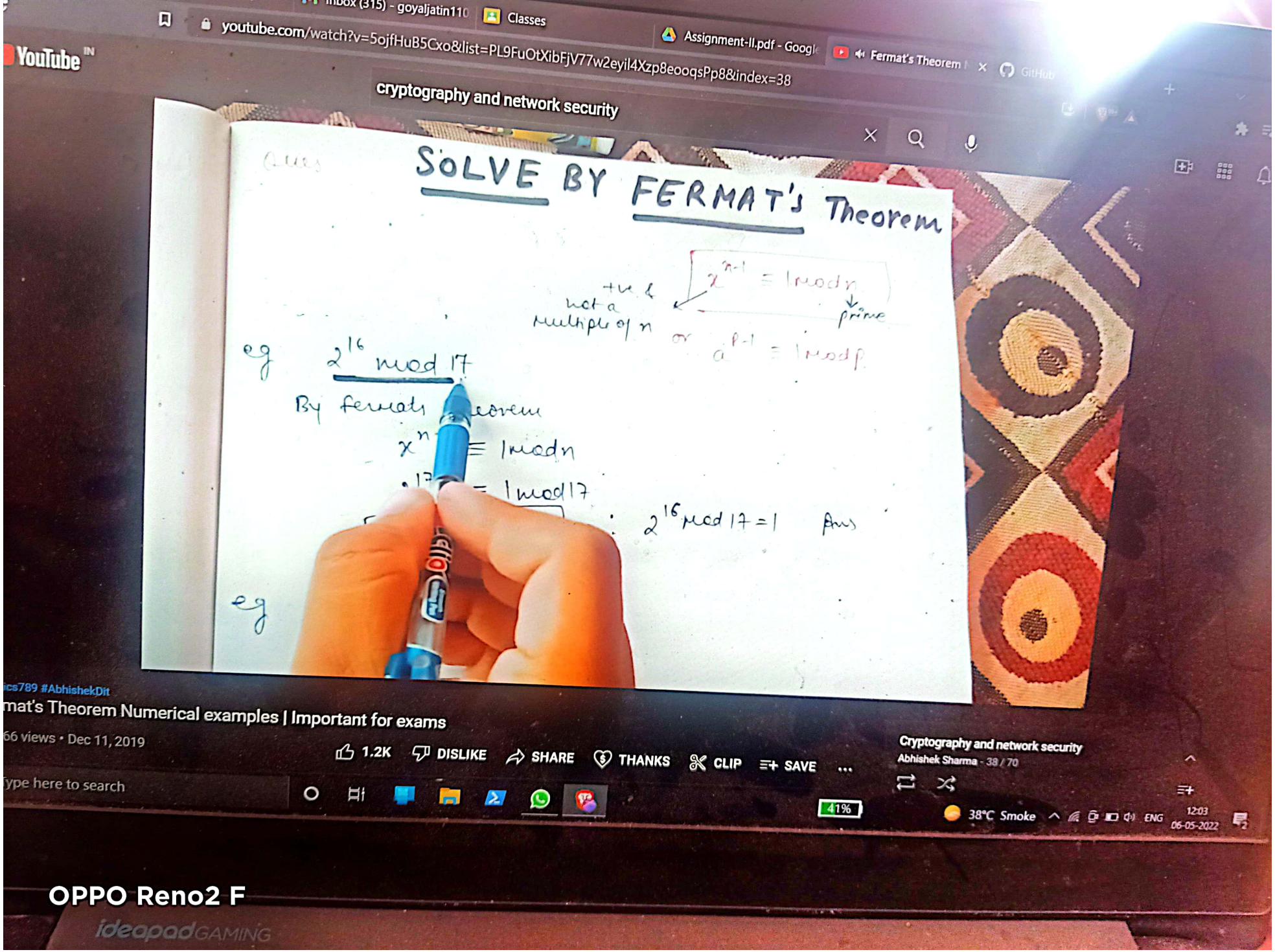
$= 29$

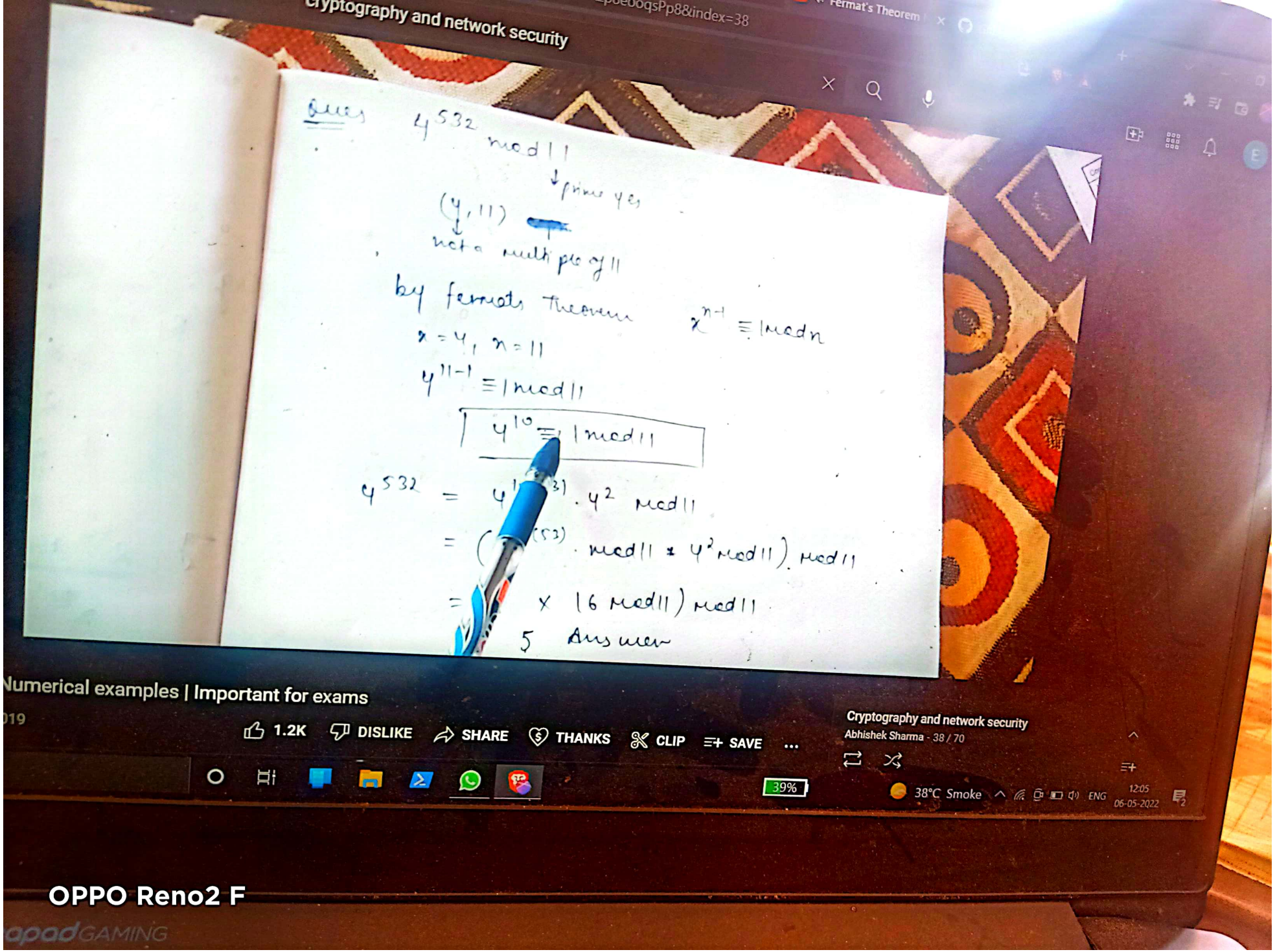
$99 \bmod 35 = 29$

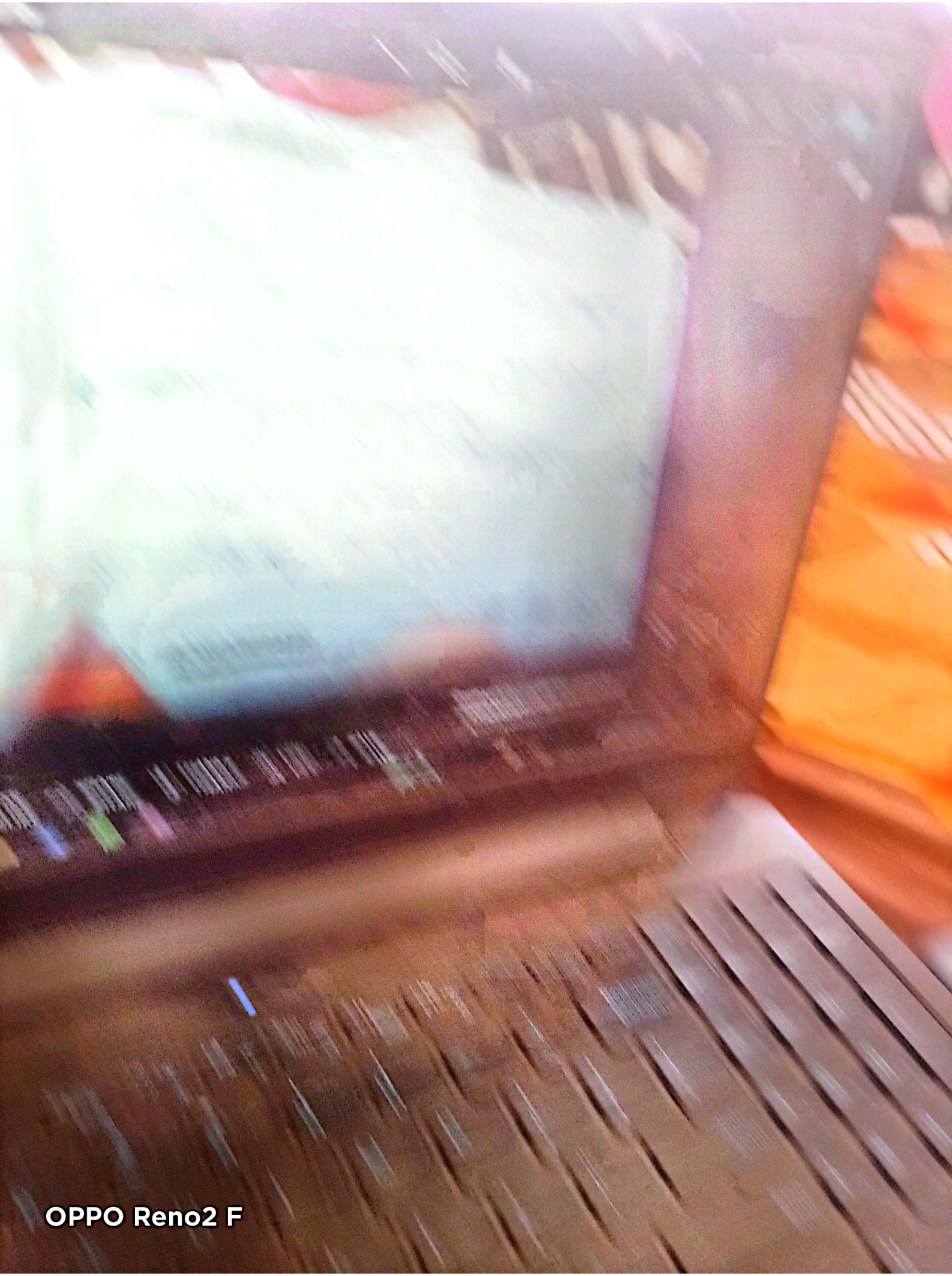
OPPO Reno2 F











# CHIENESE REMAINDER THEOREM

Chinese Remainder theorem states that there always exists an "x" that satisfies the given congruence.

$x \equiv rem[0] \pmod{num[0]}$

$x \equiv rem[1] \pmod{num[1]}$

. . . .

and $(num[0], num[1] \ldots num[n-1])$ all → must be coprime to ~~each other~~ one another.

$x \equiv 1 \bmod 5$

$\equiv 3 \bmod 7$ → 5 and 7 are coprime

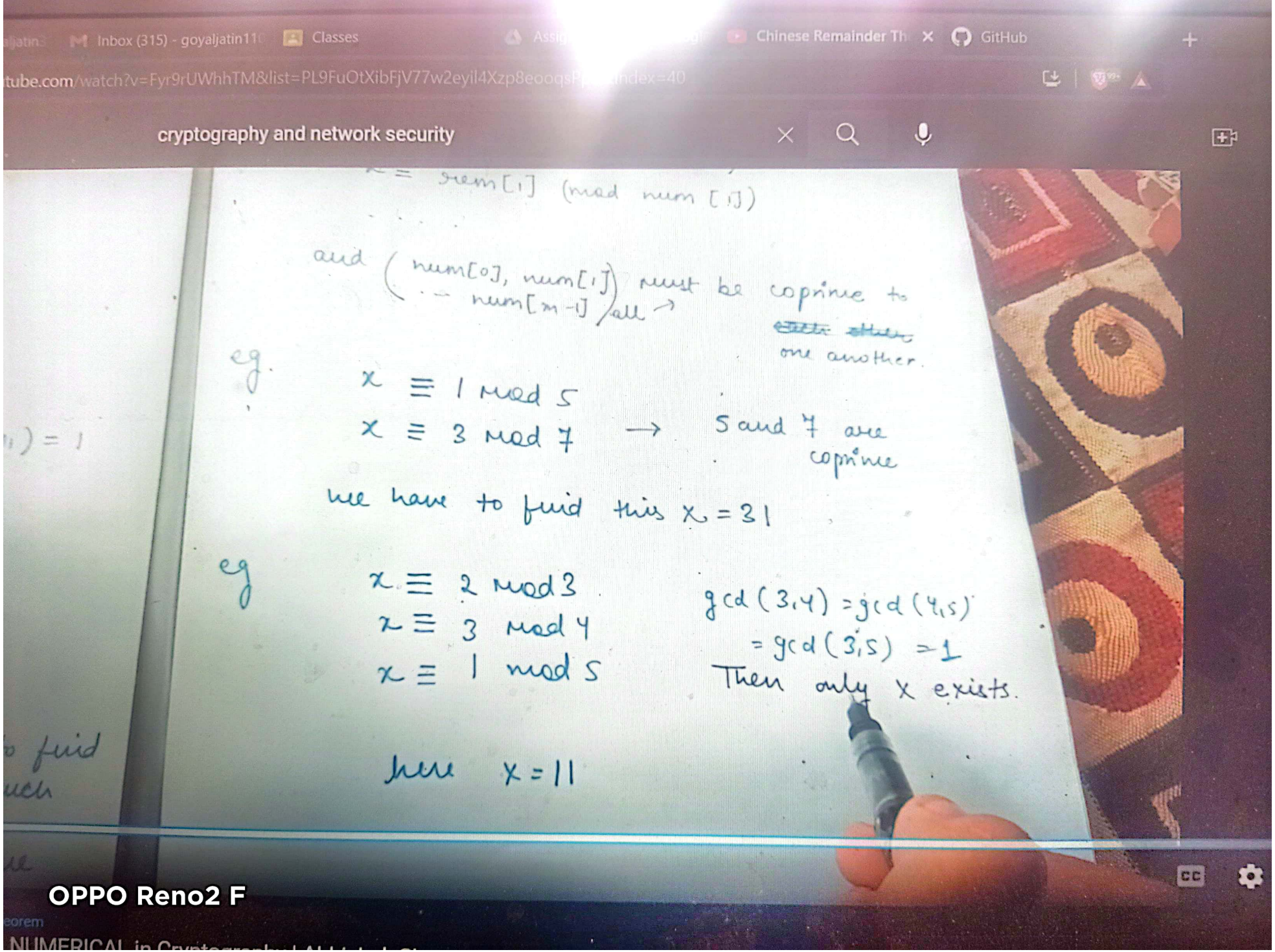
Theorem

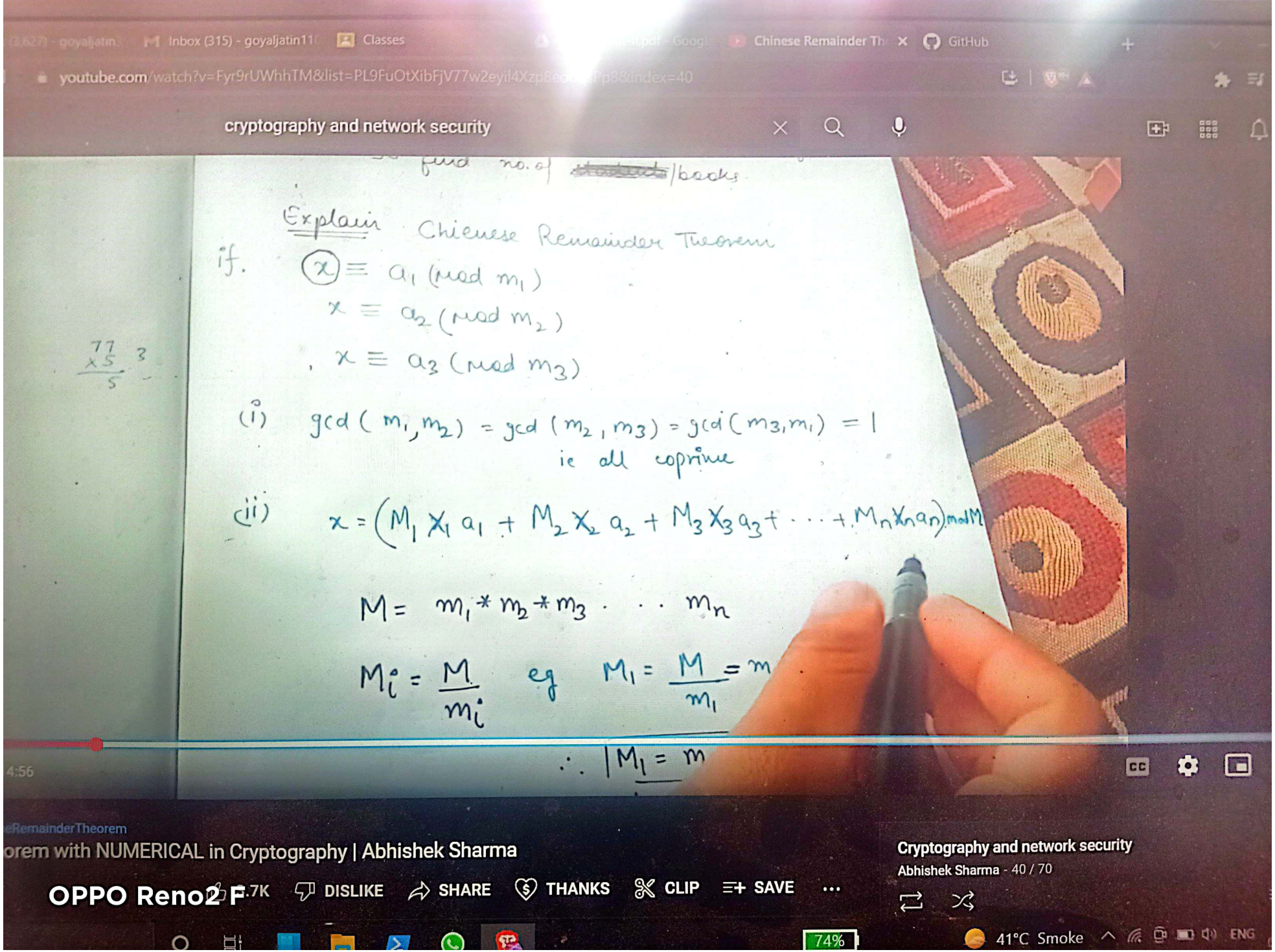
th NUMERICAL in Cryptography | Abhishek Sharma

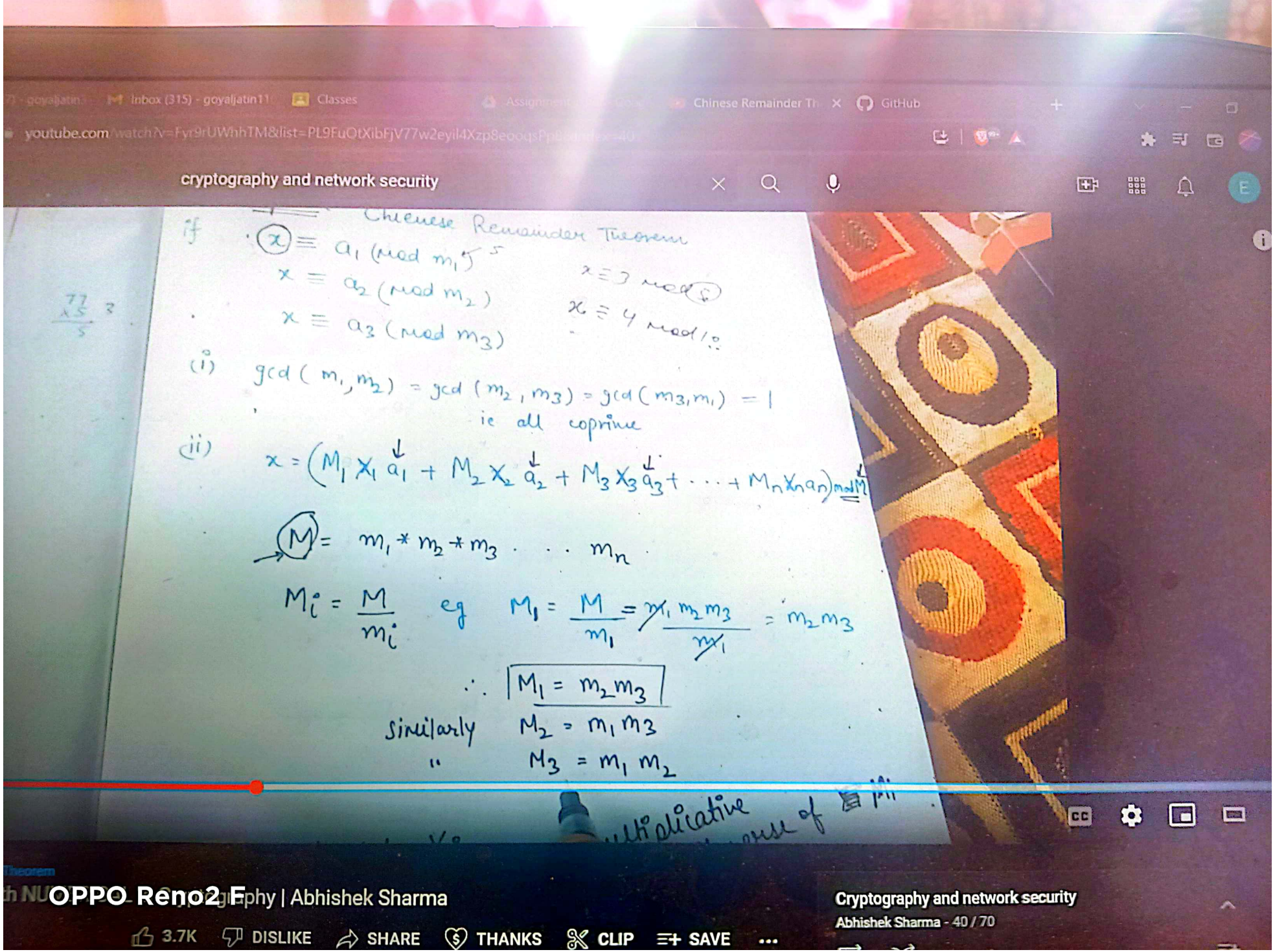
Cryptography and network security

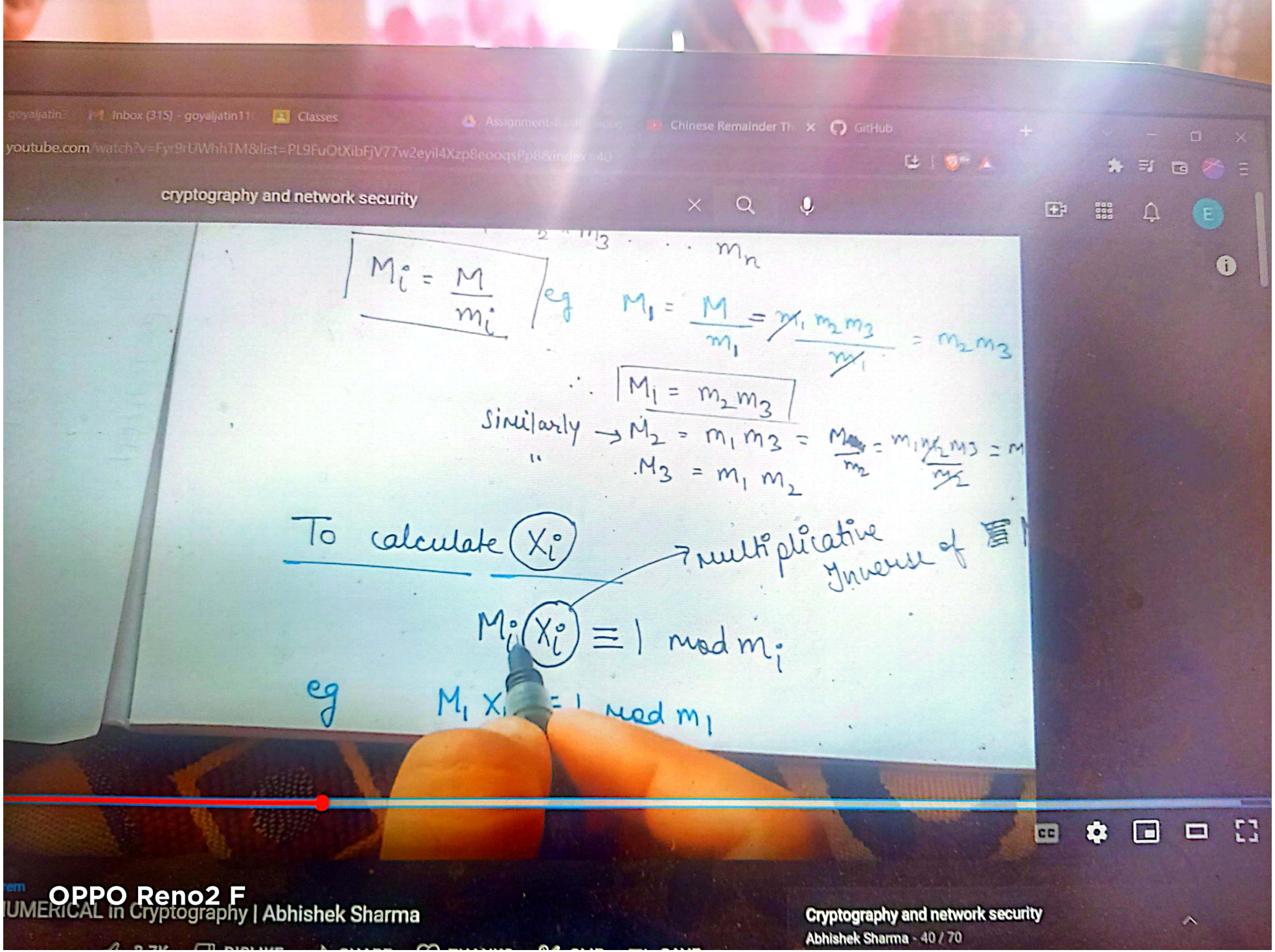
Abhishek Sharma - 40 / 70

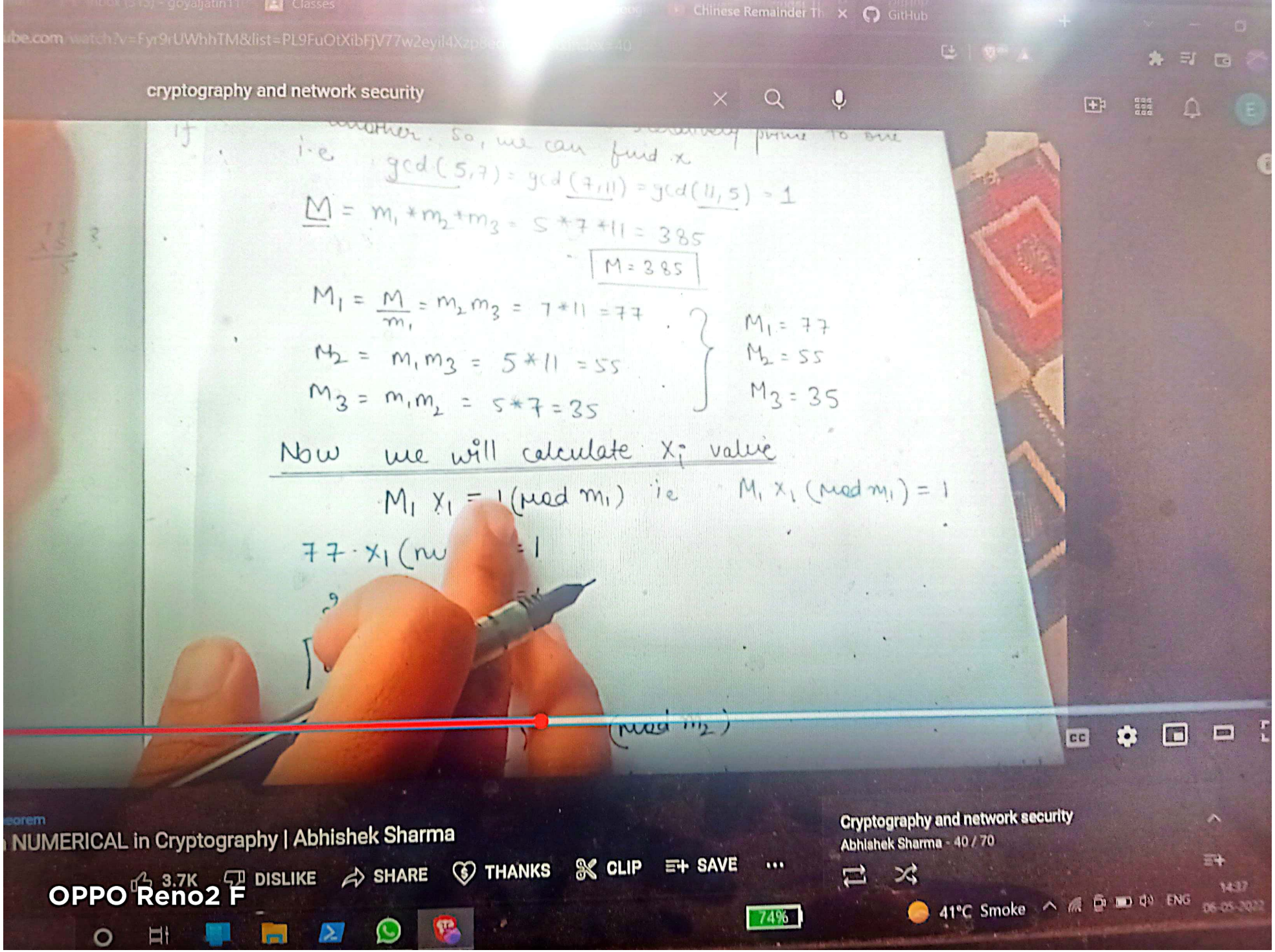
OPPO Reno2 F 3.7K DISLIKE SHARE THANKS CLIP SAVE ...

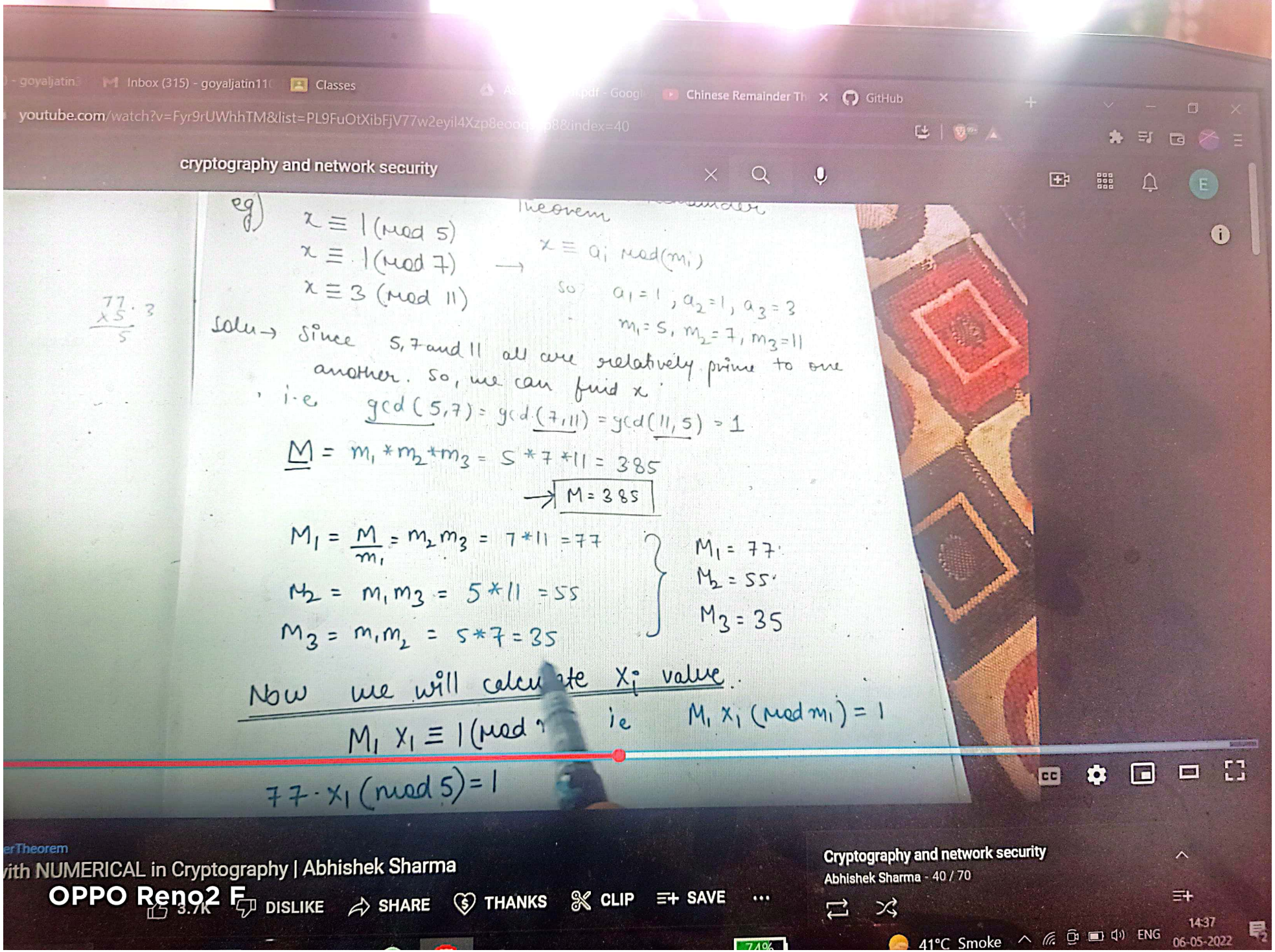


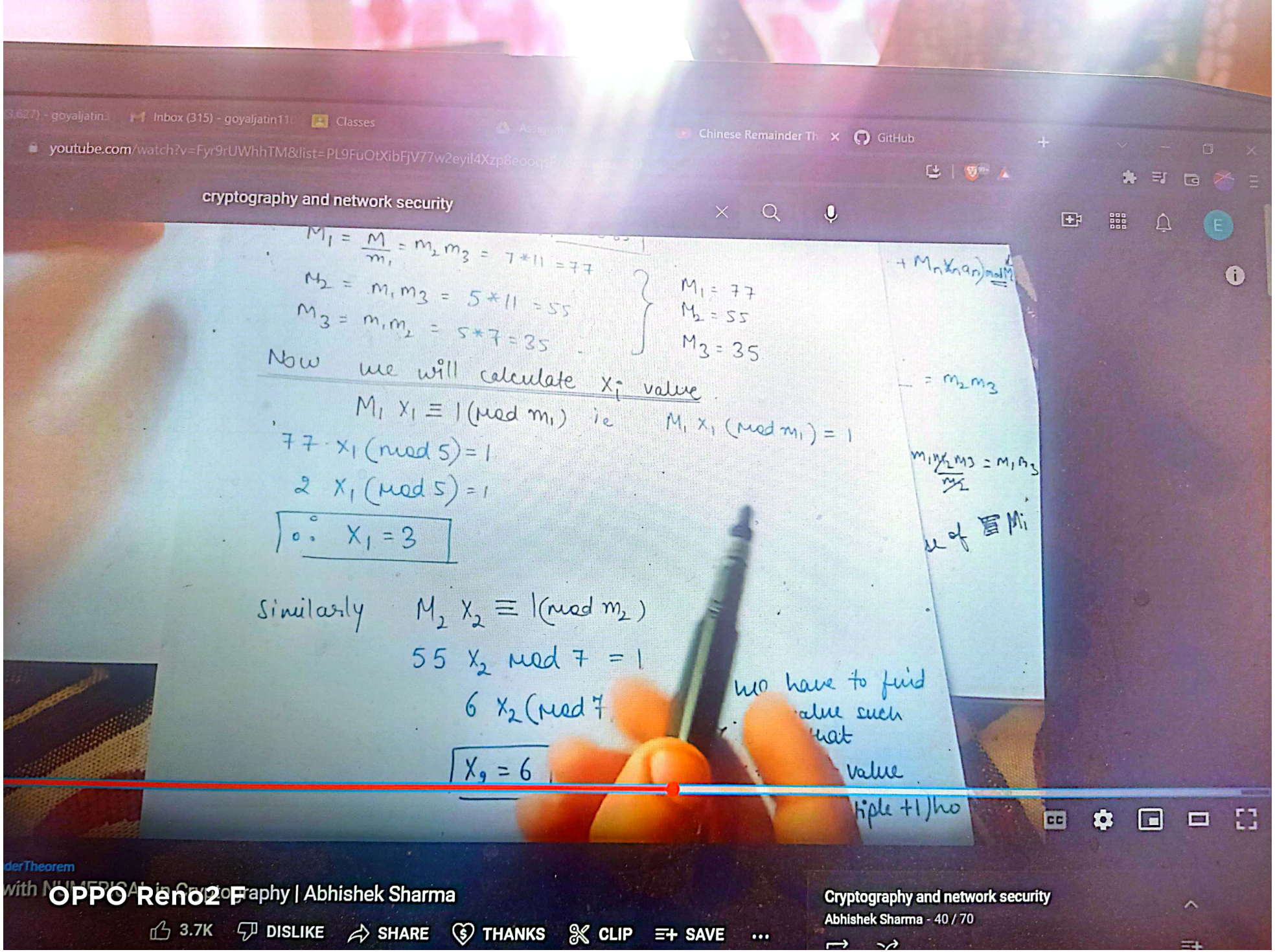


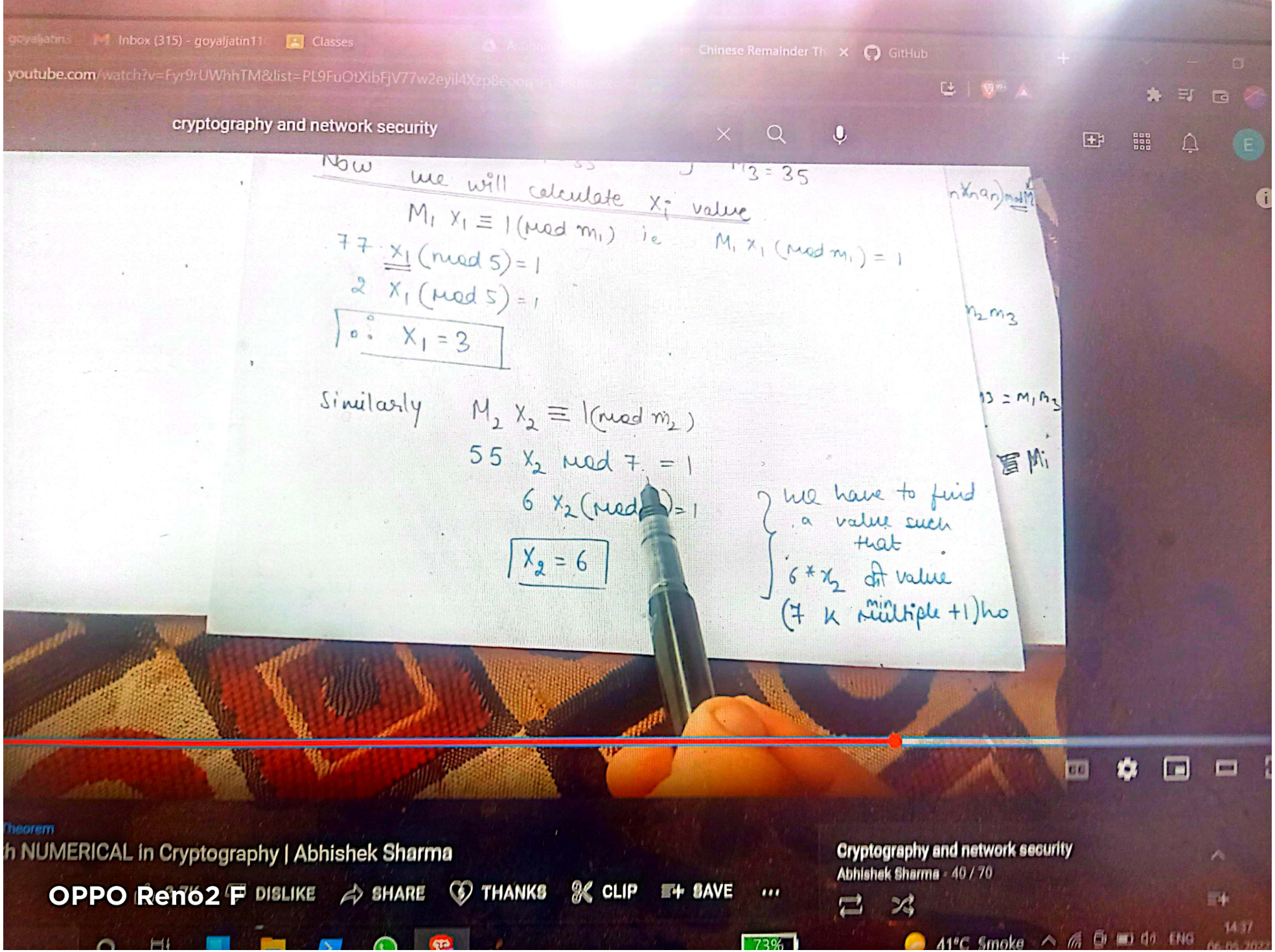


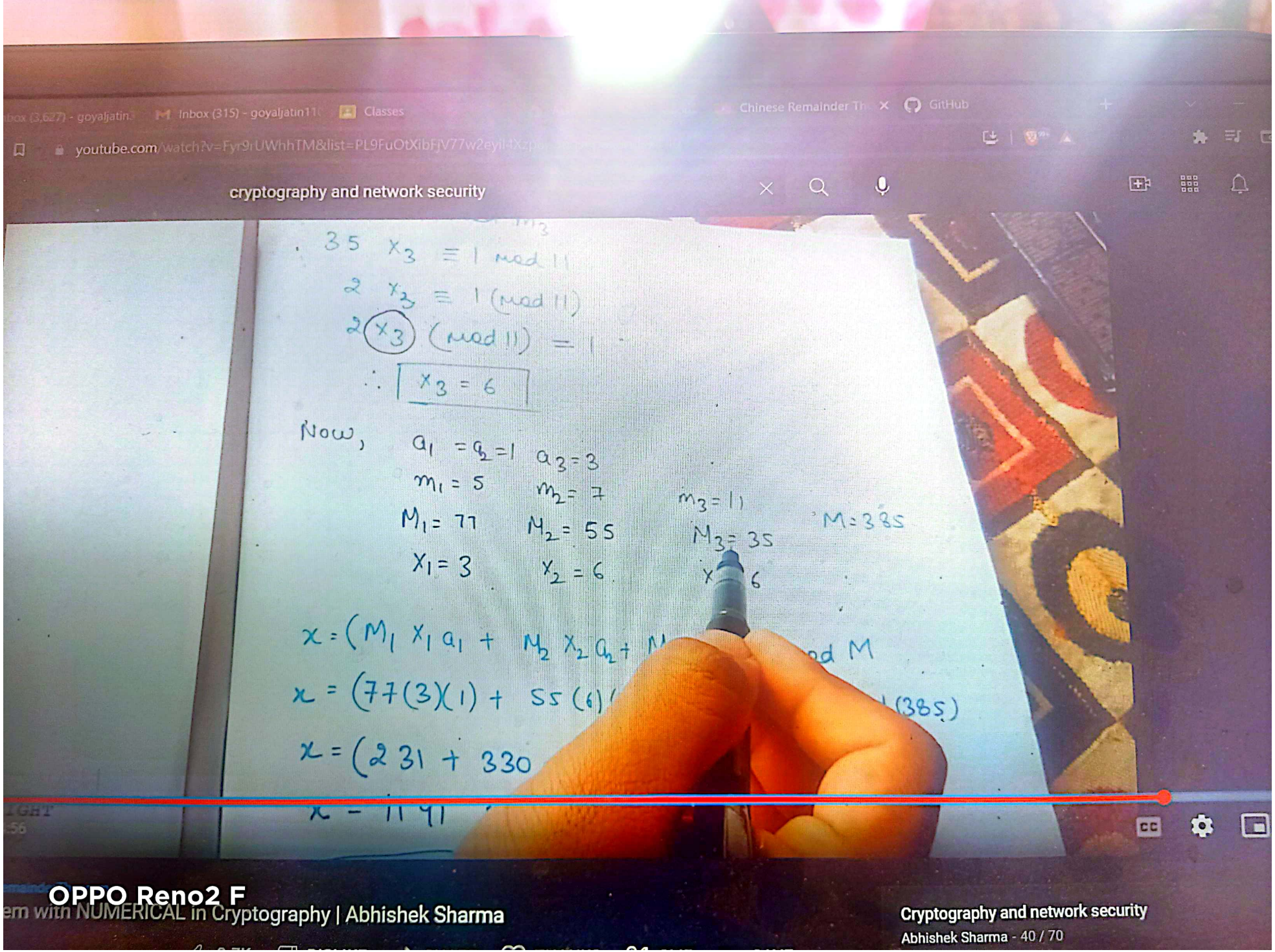












$x_3 = 6$

Now,

$a_1 = a_2 = 1$ $a_3 = 3$

$m_1 = 5$ $m_2 = 7$ $m_3 = 11$

$M_1 = 77$ $M_2 = 55$ $M_3 = 35$ $M = 385$

$X_1 = 3$ $X_2 = 6$ $X_3 = 6$

$x = (M_1 X_1 a_1 + M_2 X_2 a_2 + M_3 X_3 a_3) \bmod M$

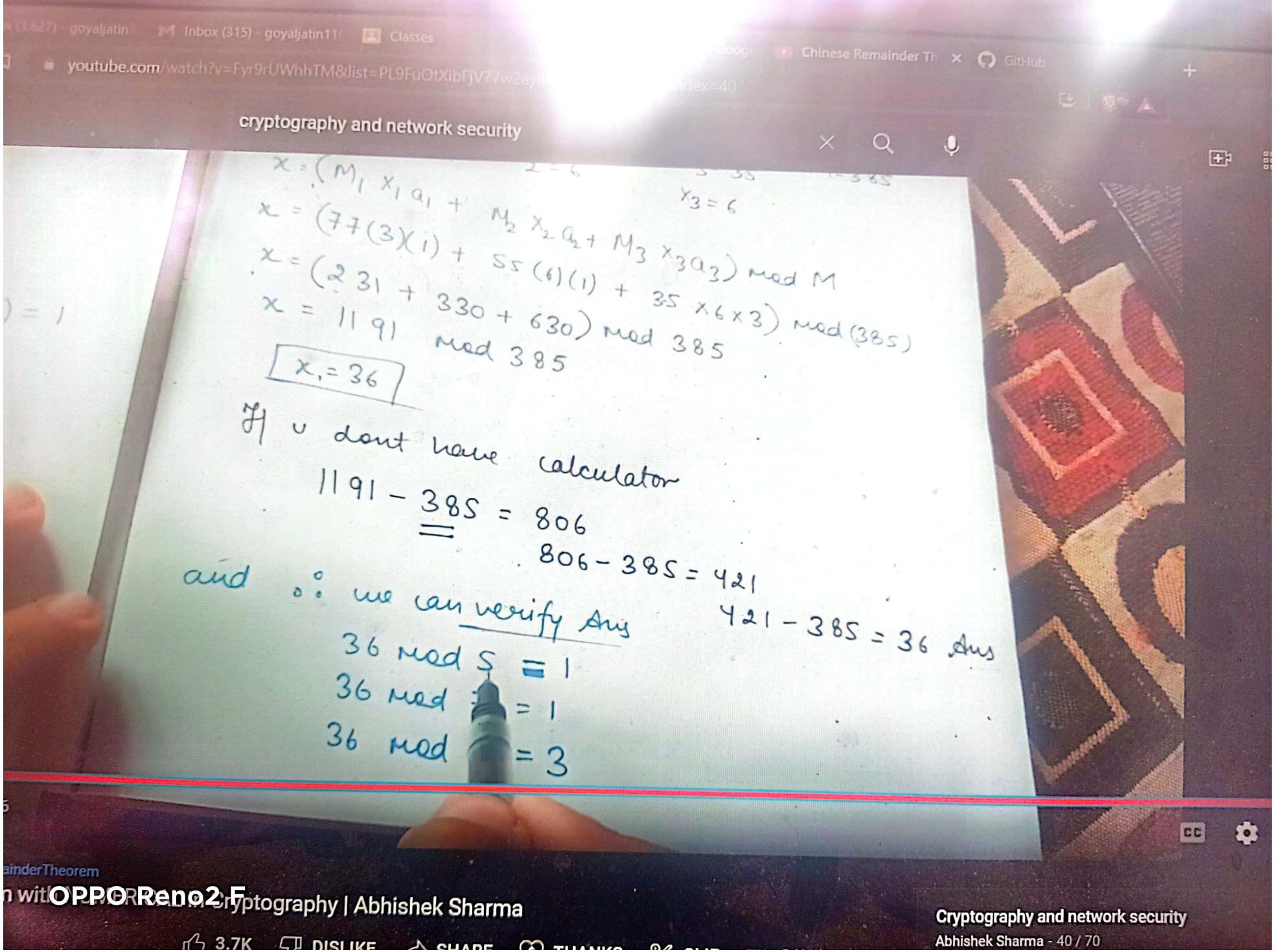
$x = (77(3)(1) + 55(6)(1) + 35 \times 6 \times 3) \bmod (385)$

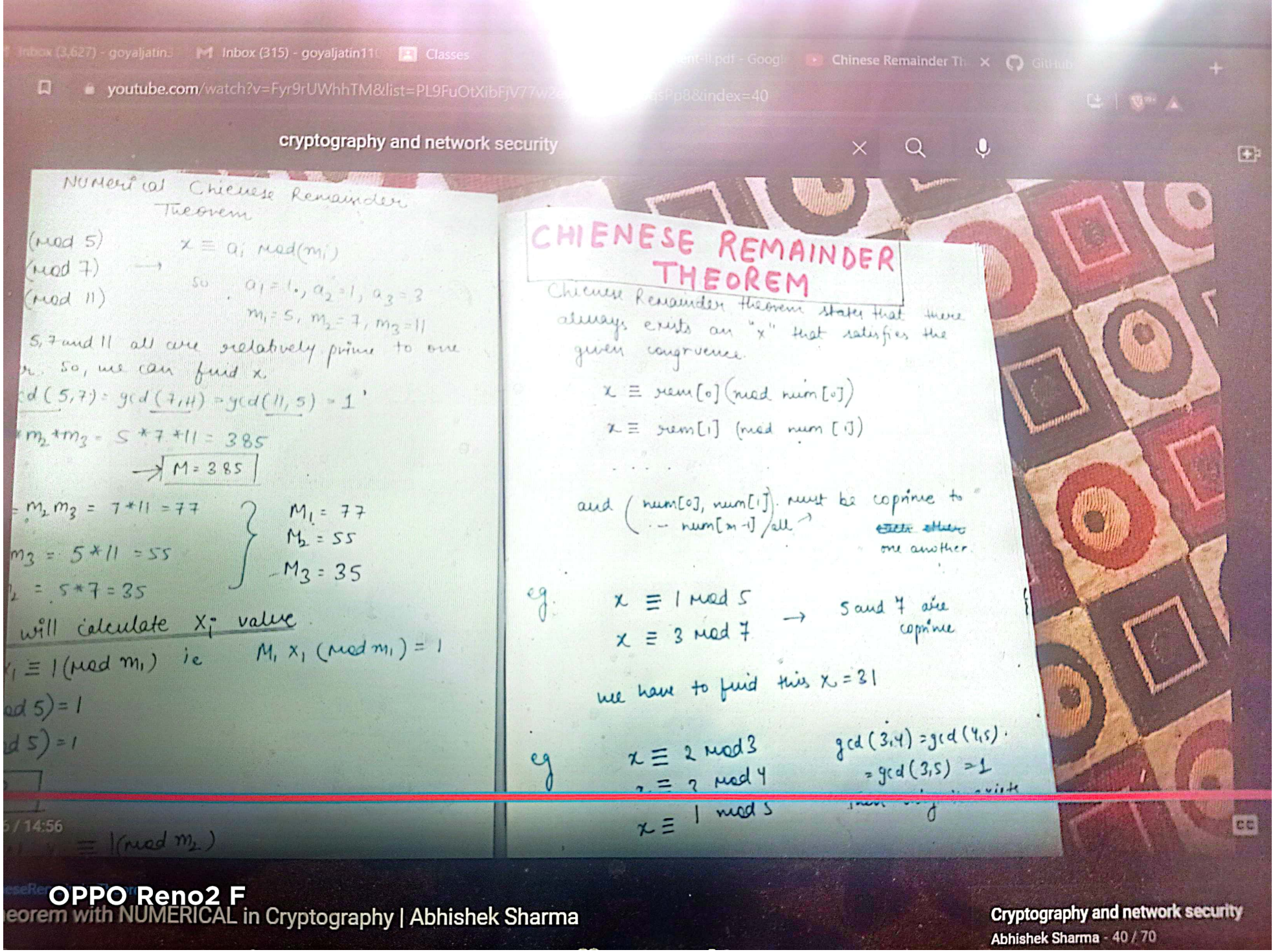
$x = (231 + 330 + 630) \bmod 385$

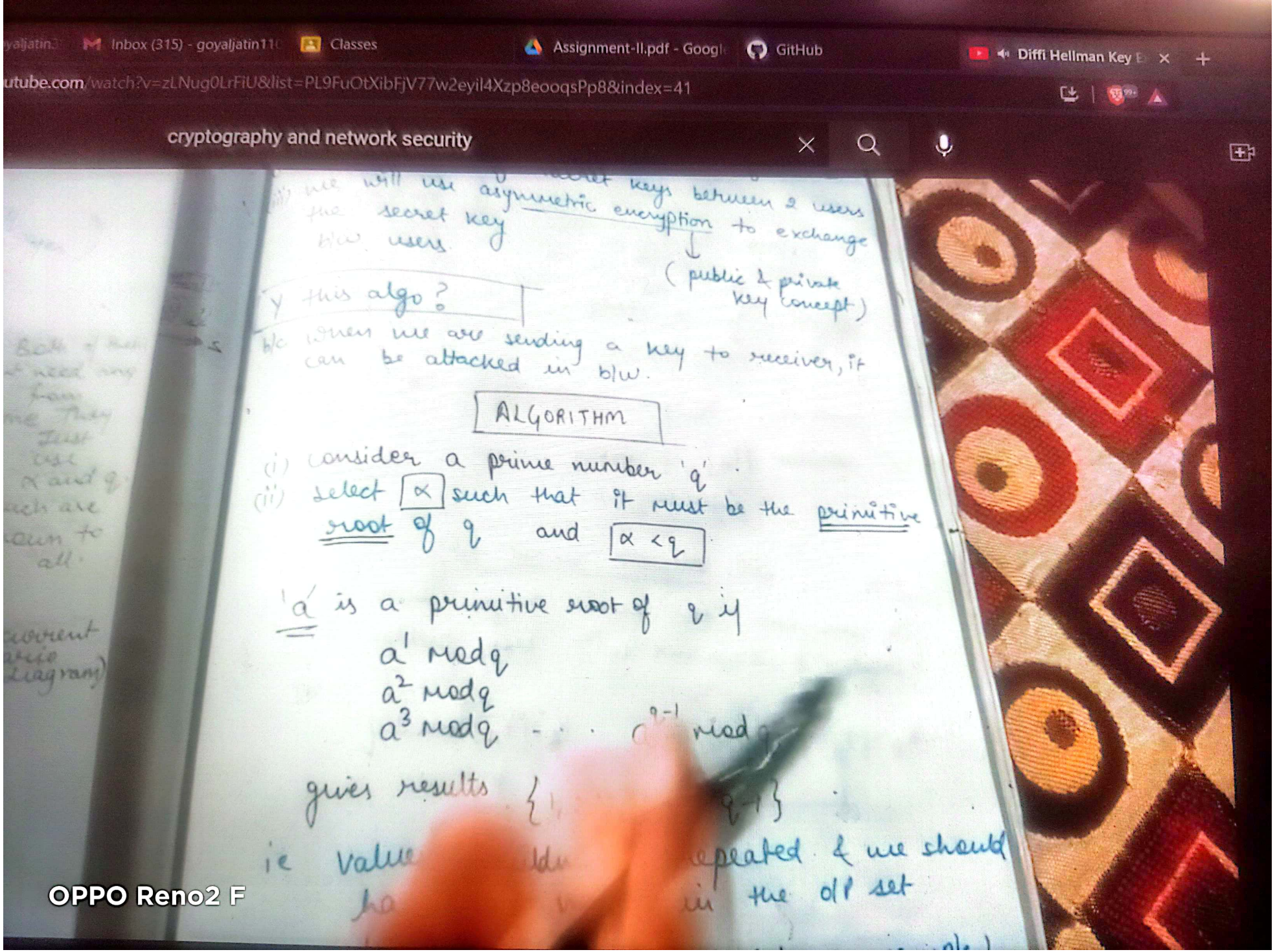
$x = 1191 \bmod 385$

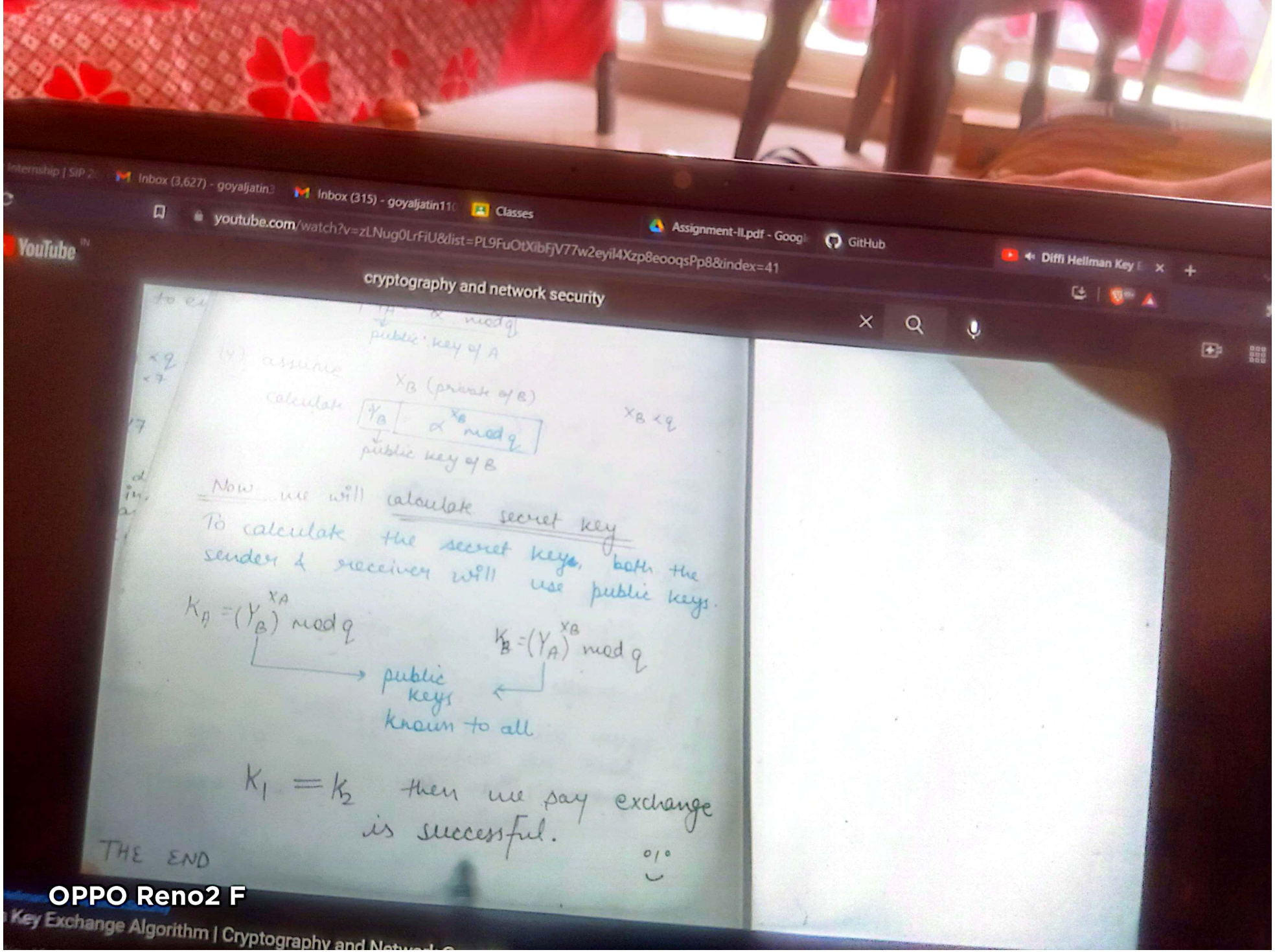
$x = 6$

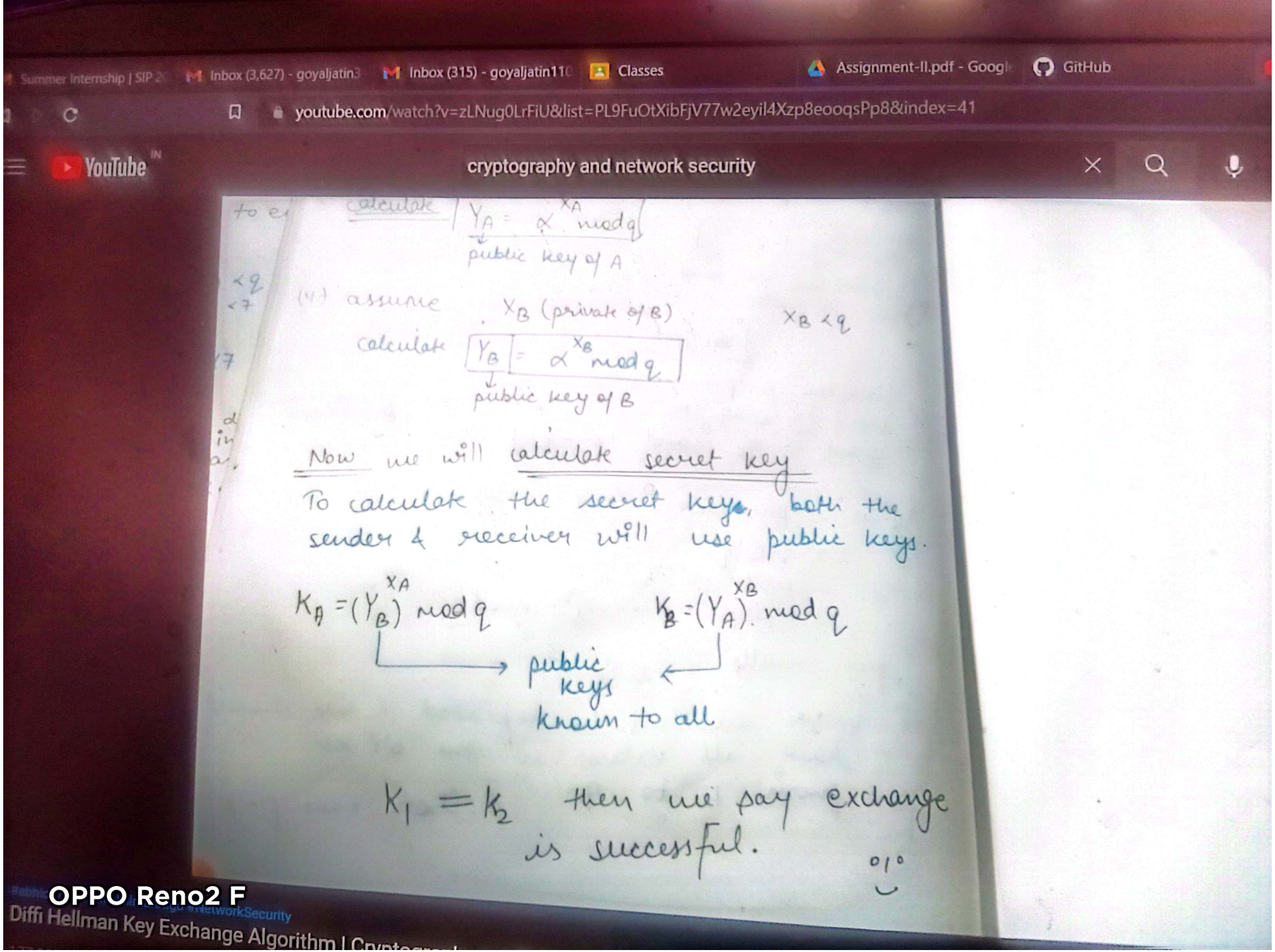
Calculator











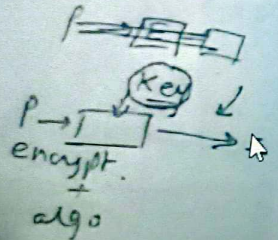
Inbox (315) - goyaljatin11 | Classes | Assignment-II.pdf - Googl | GitHub | Diffi Hellman Key Exch

tube.com/watch?v=zLNug0LrFiU&list=PL9FuOtXibFjV77w2eyil4Xzp8eooqsPp8&index=41

cryptography and network security

# Diffie-Hellman Key exchange algorithm

(i) not an encryption algo.
(ii) used to exchange secret keys between 2 users
(iii) we will use asymmetric encryption to exchange the secret key b/w users.
(public & private key concept)




Y this algo?

b/c when we are sending a key to receiver, it can be attacked in b/w.

## ALGORITHM

(i) consider a prime number 'q'
(ii) select $\alpha$ such that it must be the primitive root of q and $\alpha < q$

a is a primitive root of q if

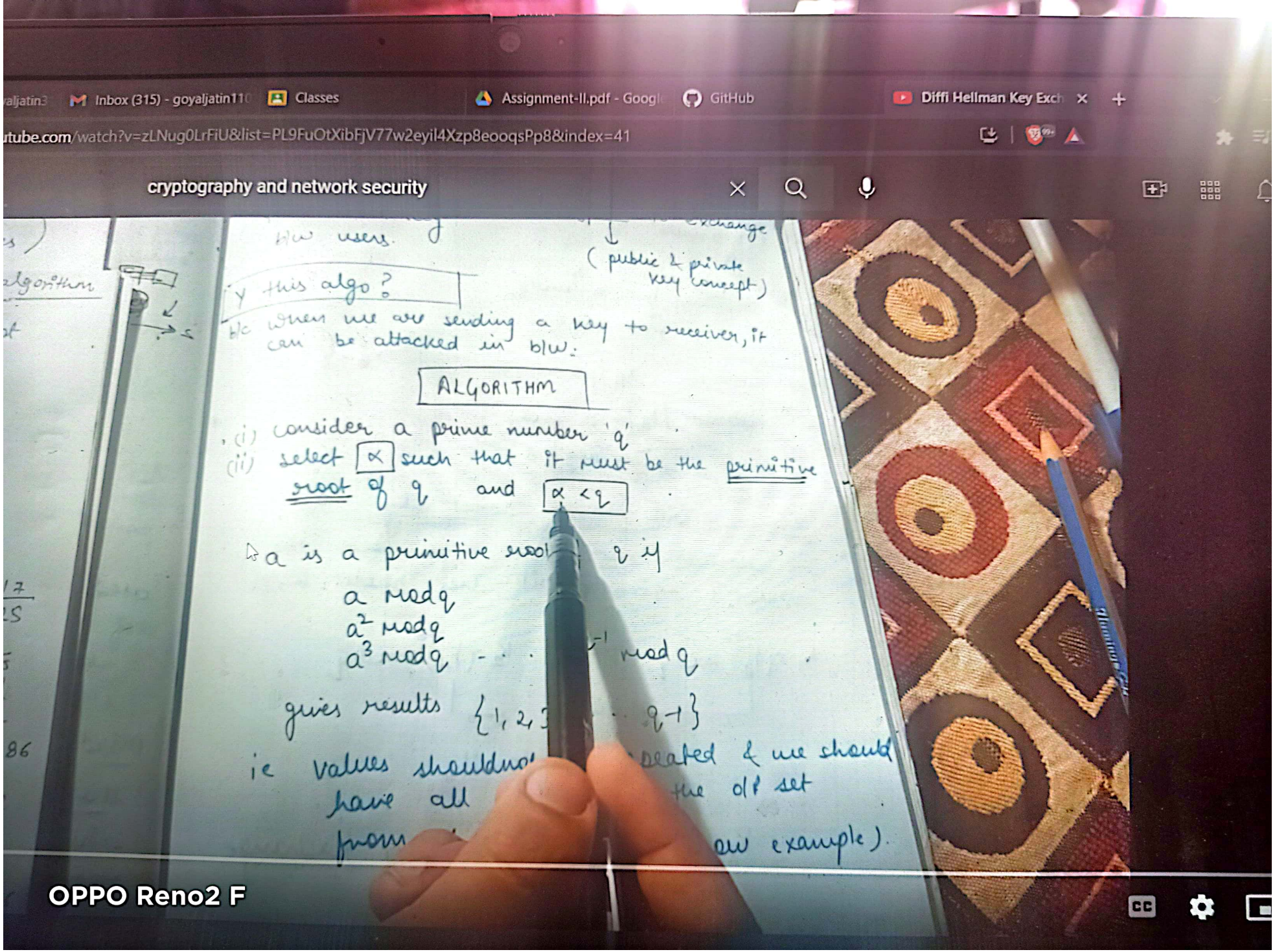
$a \bmod q$

$a^2 \bmod q$

$q-1$

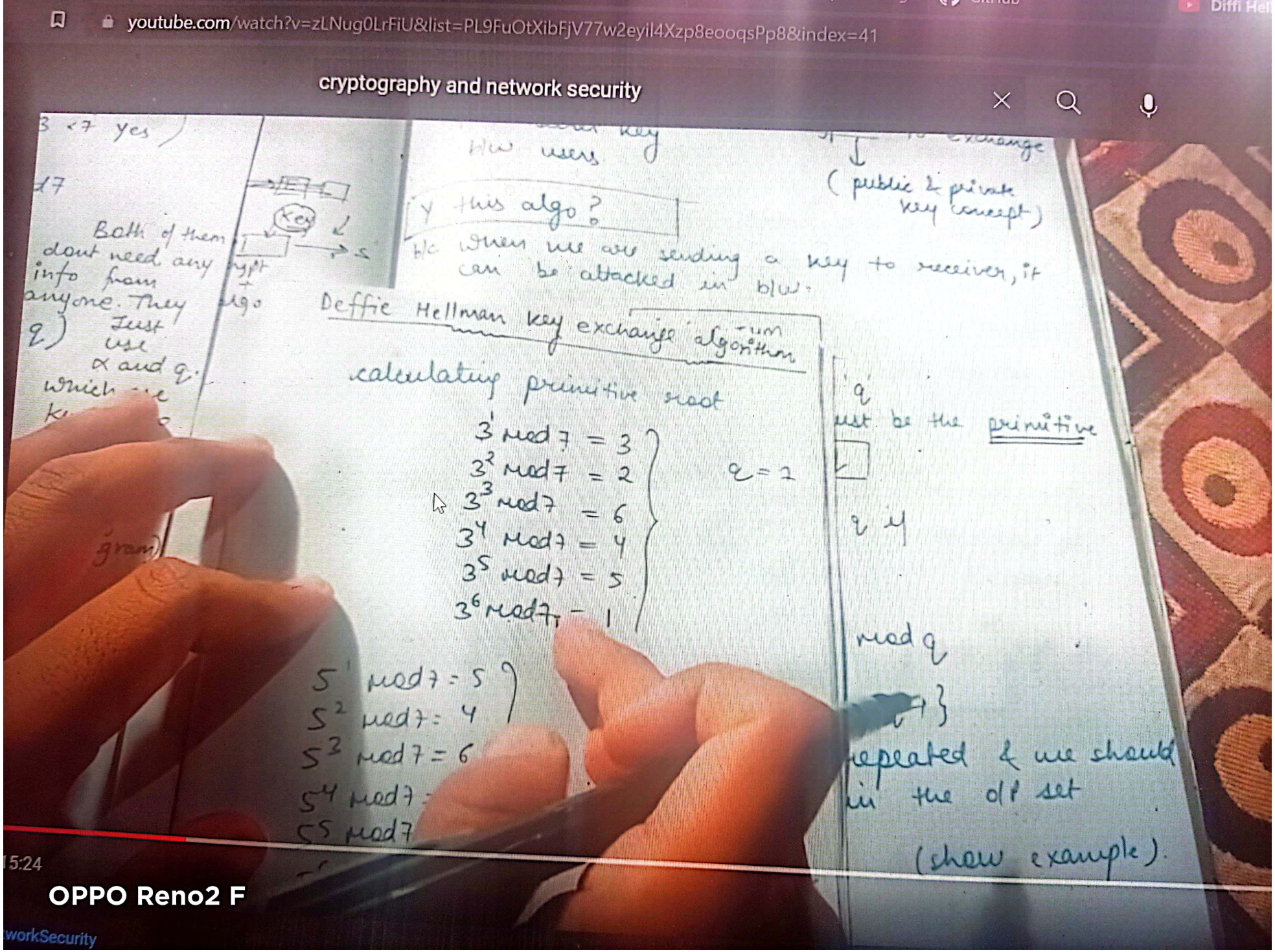
OPPO Reno2 F

Scanned with CamScanner



youtube.com/watch?v=zLNug0LrFiU&list=PL9FuOtXibFjV77w2eyil4Xzp8eooqsPp8&index=41

cryptography and network security




15:24

OPPO Reno2 F

workSecurity

om/watch?v=zLNug0LrFiU&list=PL9FuOtXibFjV77w2eyil4Xzp8eooqsPp8&index=41

cryptography and network security

Let $q = 7$ (prime)

$\alpha < q$ i.e it is a primitive root

let $\alpha = 5$ we can take any of the two primitive root 3 or 5.

$\alpha$ and $q \rightarrow$ global public elements (known to everyone)

Key generation of person1

Assume private key $X_A = 3$ ($X_A < q$, $3 < 7$ yes)

calculating public key $Y_A = \alpha^{X_A} \bmod q$

$Y_A = 5^3 \bmod 7 = 125 \bmod 7$

$Y_A = 7$

Both of them dont need any info from anyone. They just use $\alpha$ and $q$ which are known to all.

Key generation of person2

Let private key $X_B = 4$ ($X_B < q$)

calculating public key $Y_B = \alpha^{X_B} \bmod q$

$Y_B = 5^4 \bmod 7 = 2$.

$Y_B = 2$

(show current scenario diagram)

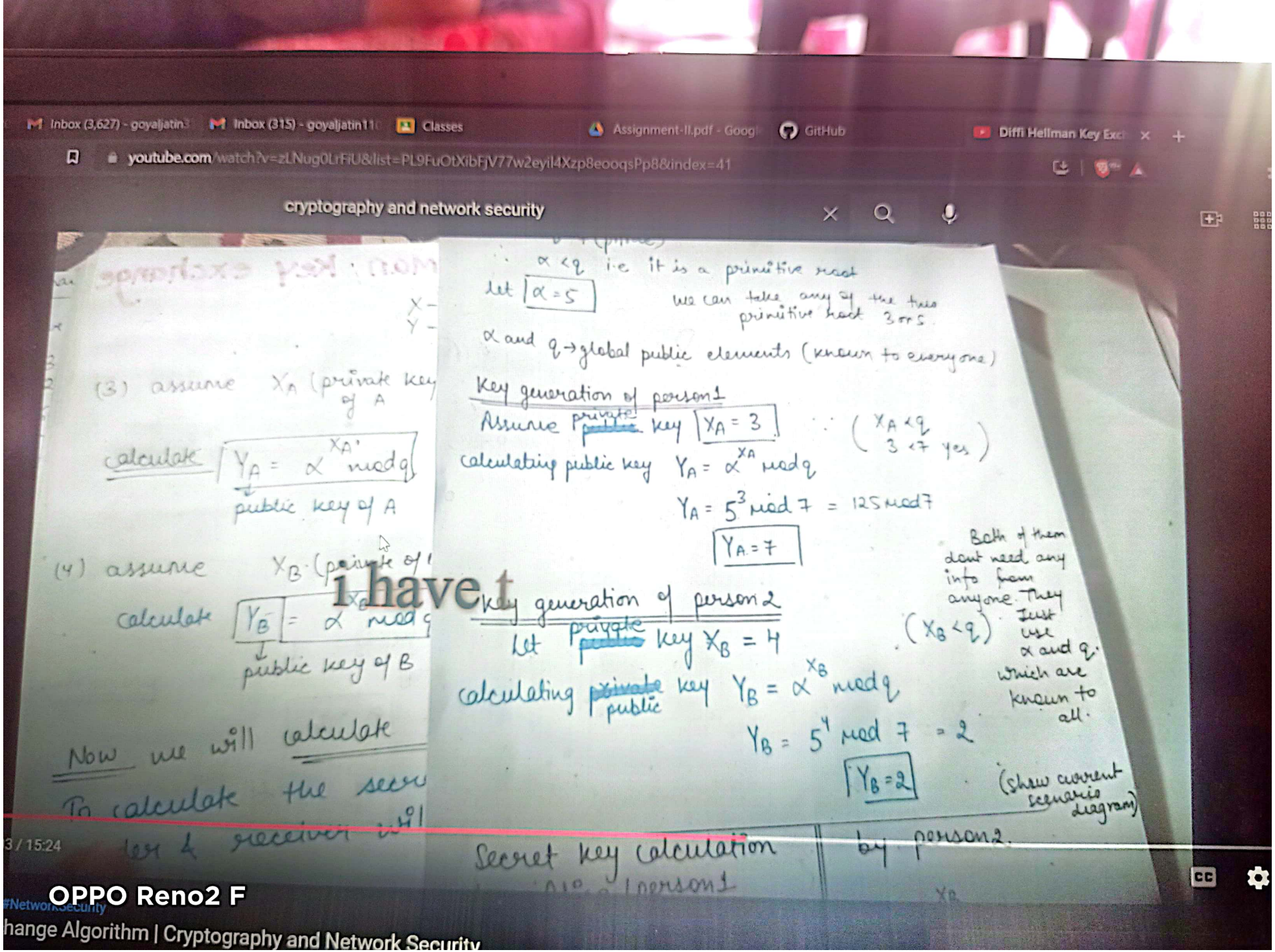
key calculation by person2

$K_2 = (Y_A)^{X_B} \bmod$

secret key

both will use

OPPO Reno2 F



cryptography and network security

Let $\alpha = 5$

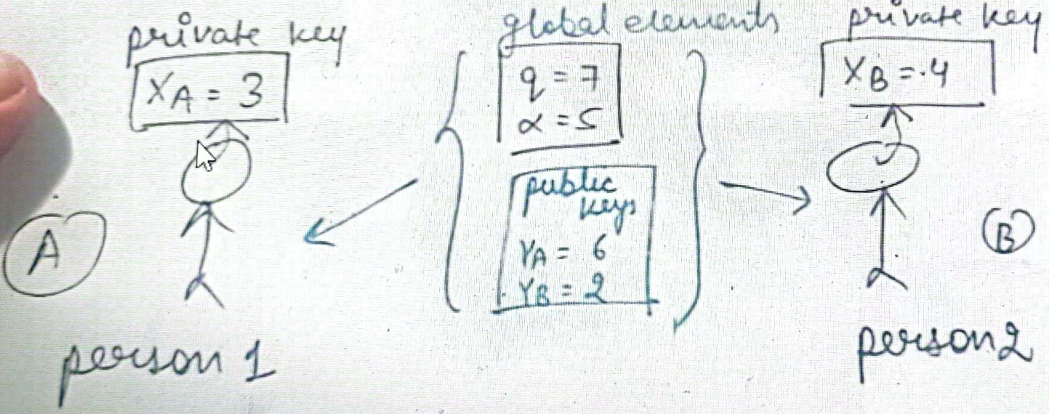
we can take any of the two primitive root 3 or 5.

$\alpha$ and $q \rightarrow$ global public elements (known to everyone)

Key generation of person1

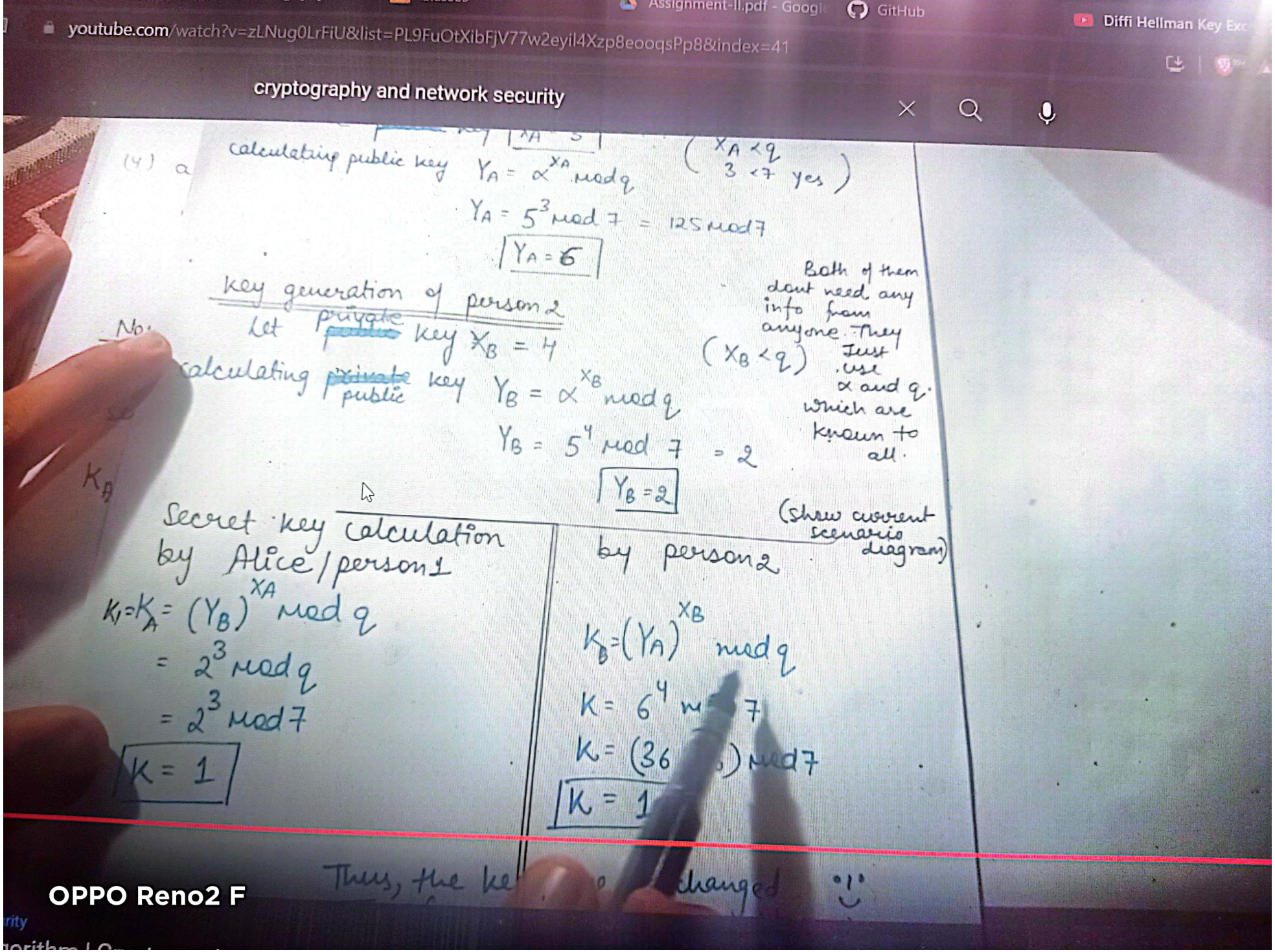
Assume private key $X_A = 3$ $\quad \because X_A < q$

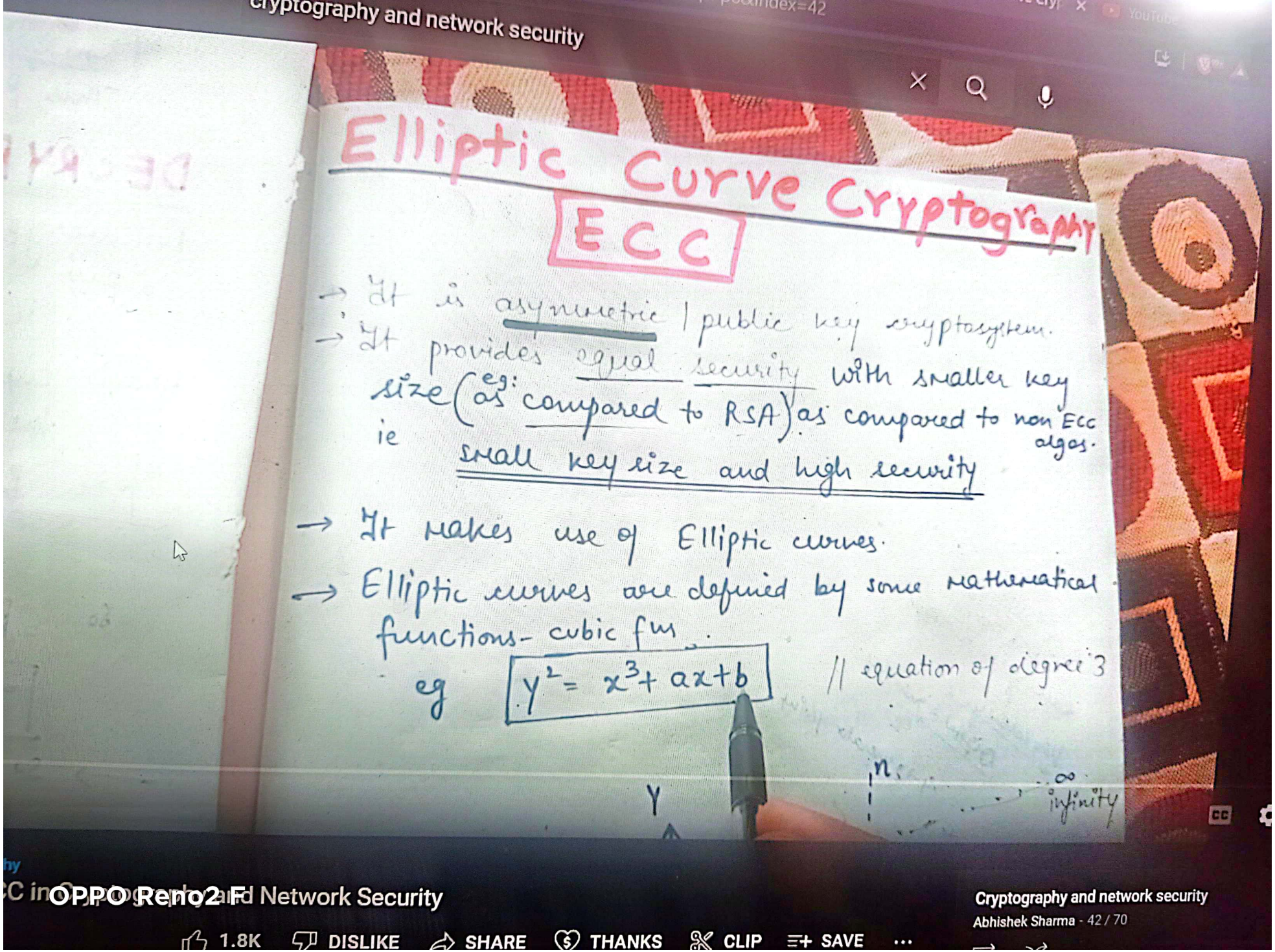
So current scenario




X → public keys

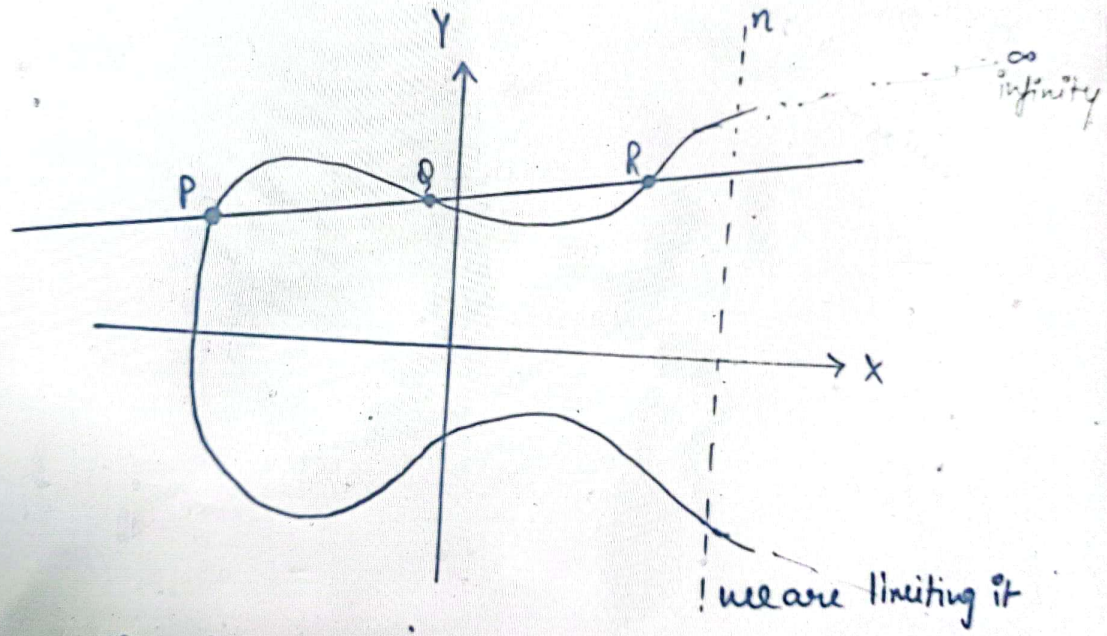
Y → private keys





functions- cubic fns

eg $y^2 = x^3 + ax + b$ // equation of degree 3

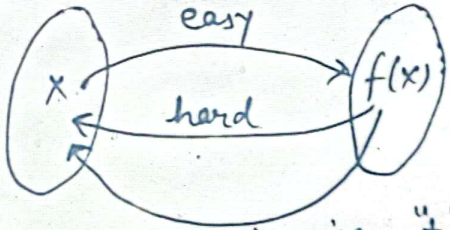



→ Symmetric to x-axis

→ If we draw a line, it will touch a max of

points

A Trapdoor function is a fn that is easy to compute in one direction, yet difficult to compute in the opposite direction (finding its inverse) without special information, called the trapdoor




easy if given "t" → trapdoor value.

A → B

Refer wikipedia for more details.

a, b

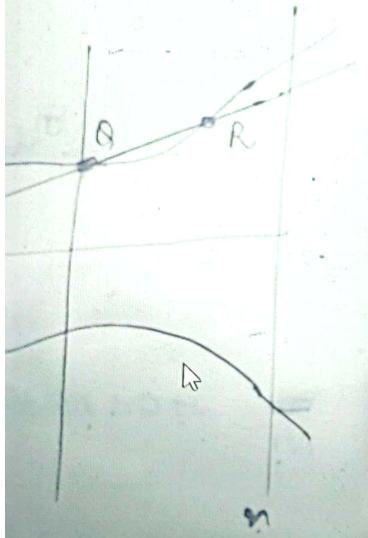
the

se

CS/IT312 Data Analytic | Assignment-II.pdf - Go | keshavagarwal17 (Kes | Elliptic Curve Cryp | YouTube

tube.com/watch?v=0NGPhAPKYv4&list=PL9FuOtXibFjV77w2eyil4Xzp8eooqsPp8&index=42

cryptography and network security




Let $E_p(a,b)$ be the elliptic curve

Consider the equation $Q = kP$

where $Q, P \rightarrow$ points on curve and $k < n$

(If k and P → given, it should be easy to find Q

but if we know Q and P, it should be extremely difficult to find k.) This is called the discrete logarithm problem for elliptic curves

ie

It is a one way fn → Trap door fn

→ P is easy

B → A

difficult..

Algo is somewhat similar ... the

Cryptography and Network Security

OPPO Reno2 F

1.8K DISLIKE SHARE THANKS CLIP SAVE ...

Cryptography and network security

Abhishek Sharma - 42 / 70

42°C Sunny ENG 18:19 06-05-2022

# ECC - ALGORITHM

## ECC - Key Exchange

### Global Public Elements

$E_q(a,b)$ : elliptic curve with parameters $a, b$ and $q$

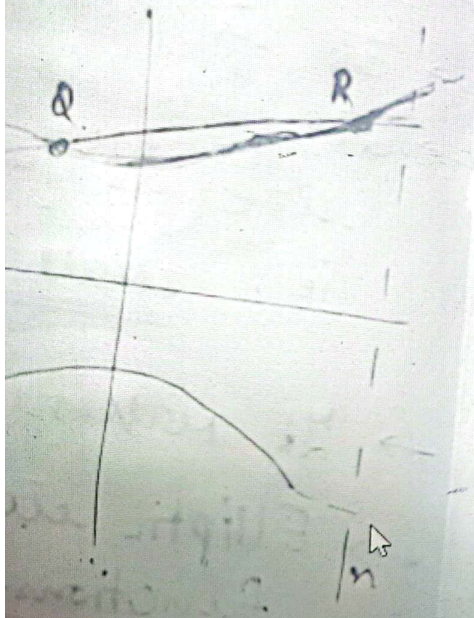
$q$ → prime no. or an integer of the form $2^m$.

$G$ : Point on the curve/elliptic curve whose order is large value of $n$

### User A key generation

Select private key $n_A < n$

calculate public key $P_A$ $\quad P_A = n_A \times G$



$E_q(a,b)$ : elliptic curve with parameters $a, b$ and $q$

$q$ → prime no. or an integer of the form $2^m$.

$G$: Point on the curve/elliptic curve whose order is large value of $n$

**User A key generation**

Select private key $n_A$ $\quad n_A < n$

calculate public key $P_A$ $\quad P_A = n_A \times G$

**User B key generation**

select private key $n_B$ $\quad n_B < n$

calculate public key $P_B$ $\quad P_B = n_B \times G$

**Calculation of secret key by**

$K = n_A \times P_B$

elliptic curve with parameters a, b and [q]

↓

prime no or an integer of the form $2^m$.

**G:** Point on the curve/elliptic curve whose order is large value of n

**User A key generation**

Select private key $n_A$ $\quad n_A < n$

calculate public key $P_A$ $\quad P_A = n_A \times G$

**User B key generation**

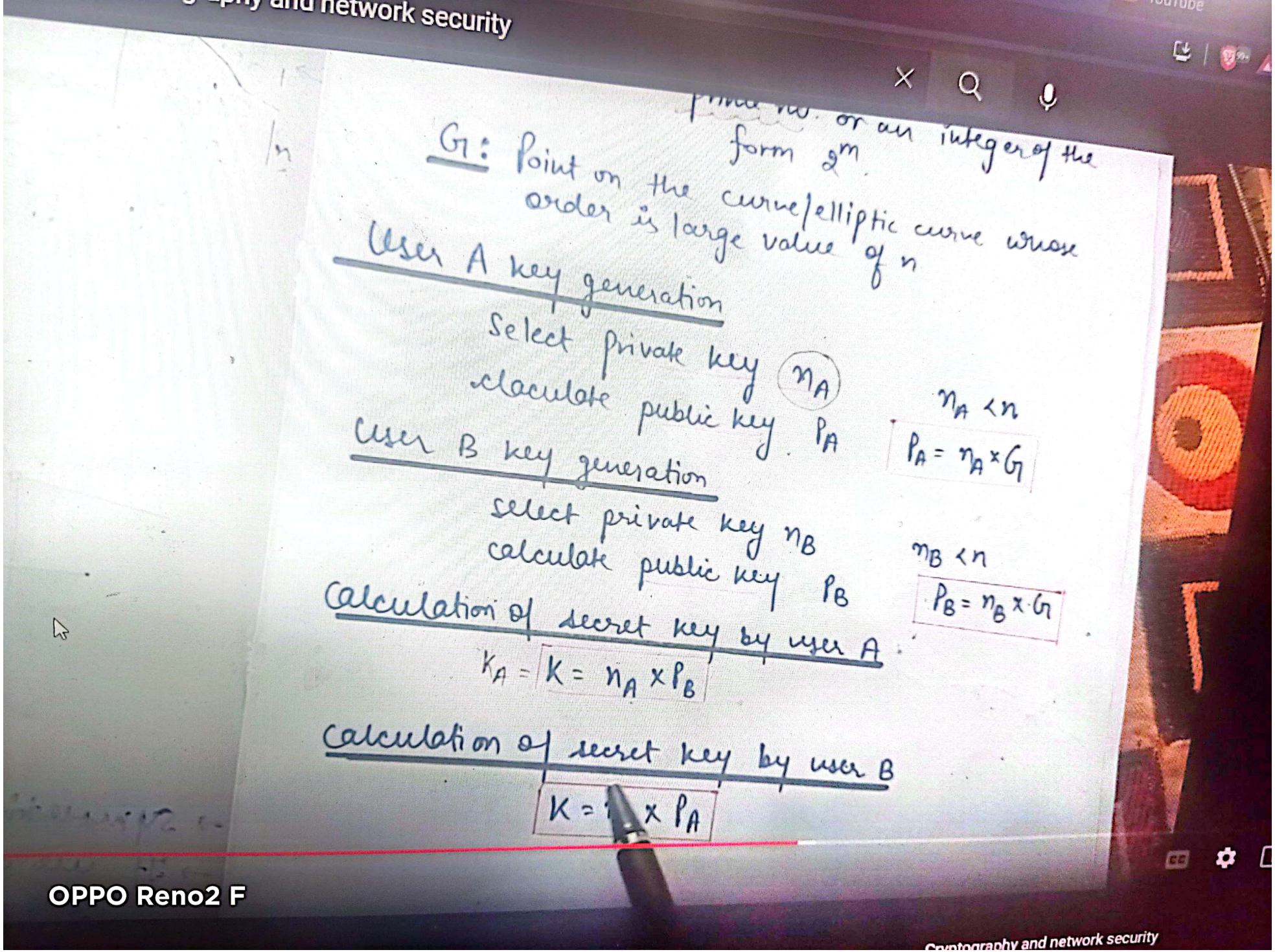
select private key $n_B$ $\quad n_B < n$

calculate public key $P_B$ $\quad P_B = n_B \times G$

**Calculation of secret key by ... A**

$K = n_A \times P_B$

**Calculation of secret ...**



# ECC ENCRYPTION

- Let the message be M.
- First encode this message M into a point on elliptic curve.
- Let this point be $P_m$.

Now this point is encrypted.

The cipher point will be

$$C_m = \{kG, P_m + kP_B\}$$

This point will be sent to the receiver

# DECRYPTION

for decryption, multiply 1st point in the

The cipher point will be

$$C_m = \{kG, P_m + kP_B\}$$

This point will be sent to the receiver

## DECRYPTION

for decryption, multiply 1st point in the pair with receiver's secret key

ie $kG * n_B$

Then subtract it from 2nd point/coordinate in the pair

i.e. $P_m + kP_B - (kG * n_B)$

but we know $P_B = n_B \times G$

So $= P_m + kP_B - kP_B$

$= P_m$ (original

→ So receiv

A → B

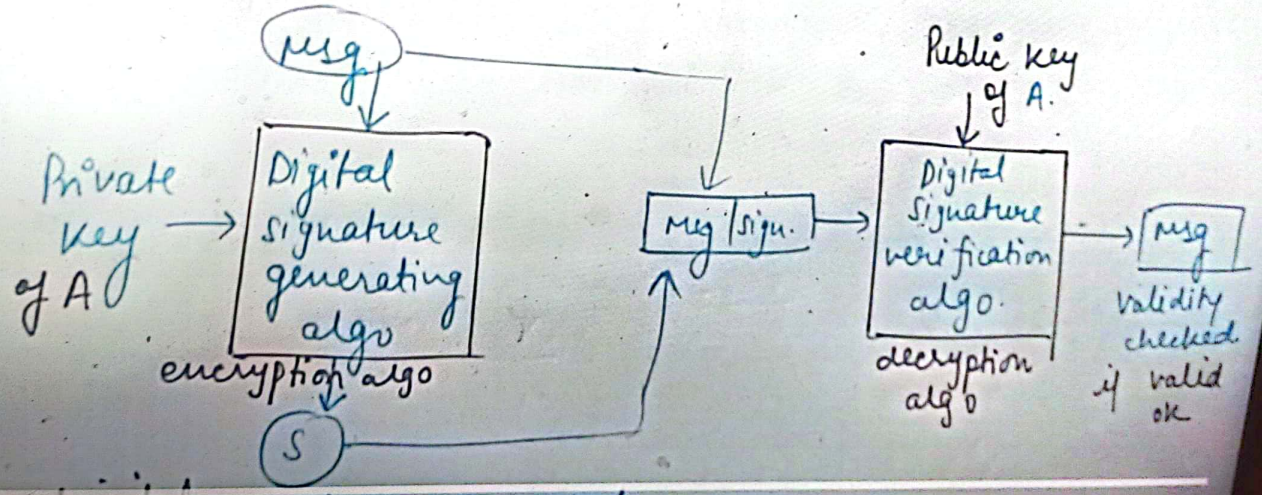
# Digital Signature

→ vimp role in e-commerce, online transaction, etc.

→ based on asymmetric key cryptography
encryption → private key
decryption → public key

→ used for msg authentication & non repudiation & msg integrity

→ not used for confidentiality




digital signature generated

nature

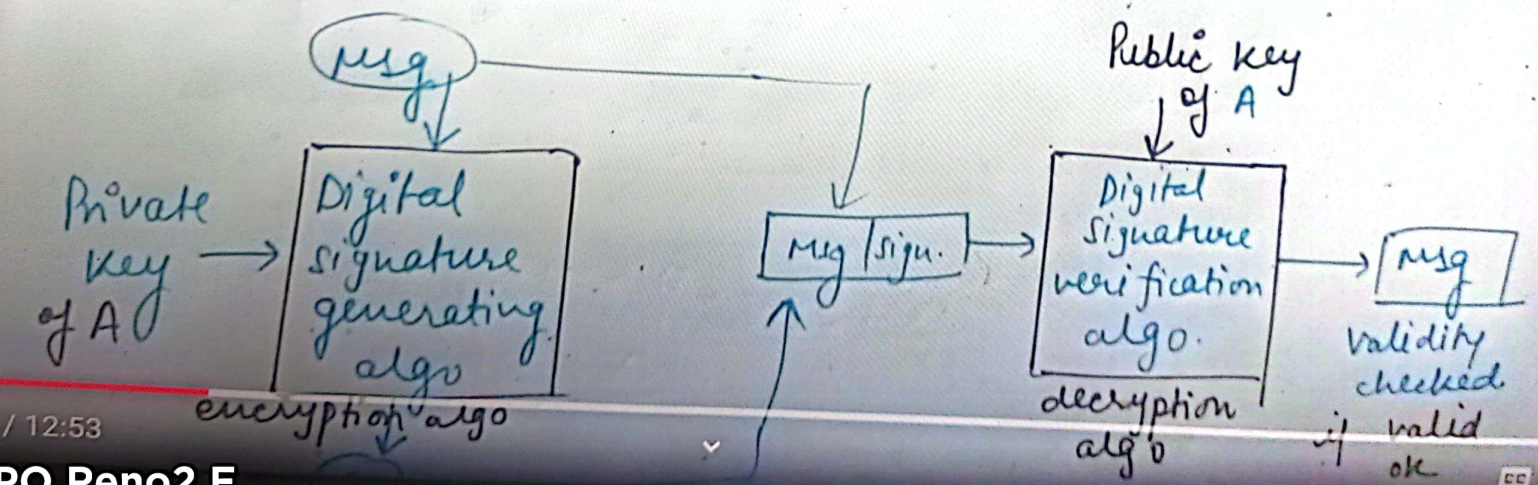
# Digital Signature

→ vimp role in e-commerce, online transaction, etc.

→ based on asymmetric key cryptography
encryption → private key
decryption → public key

→ used for msg authentication & non repudiation & msg integrity

→ not used for confidentiality




3:31 / 12:53

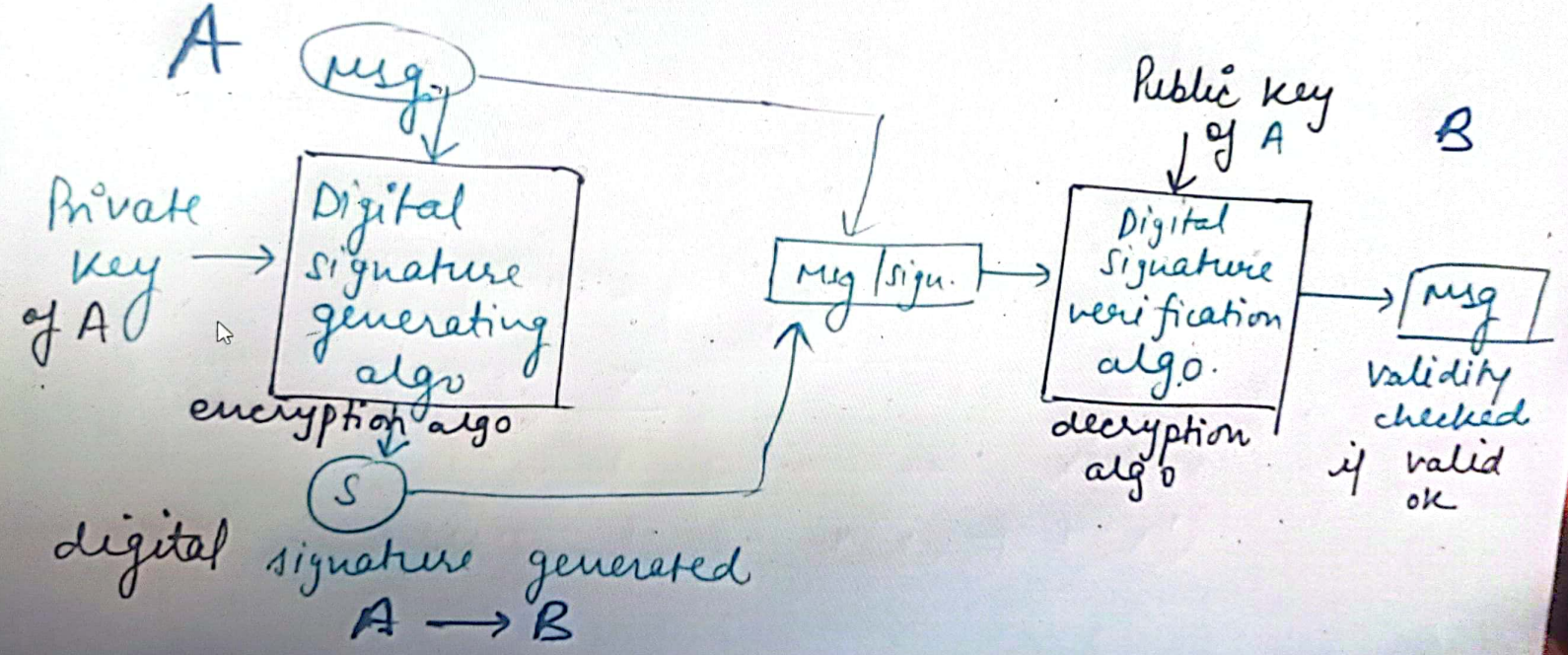
OPPO Reno2 F

decryption → private key

decryption → public key

→ used for msg authentication & non repudiation & msg integrity

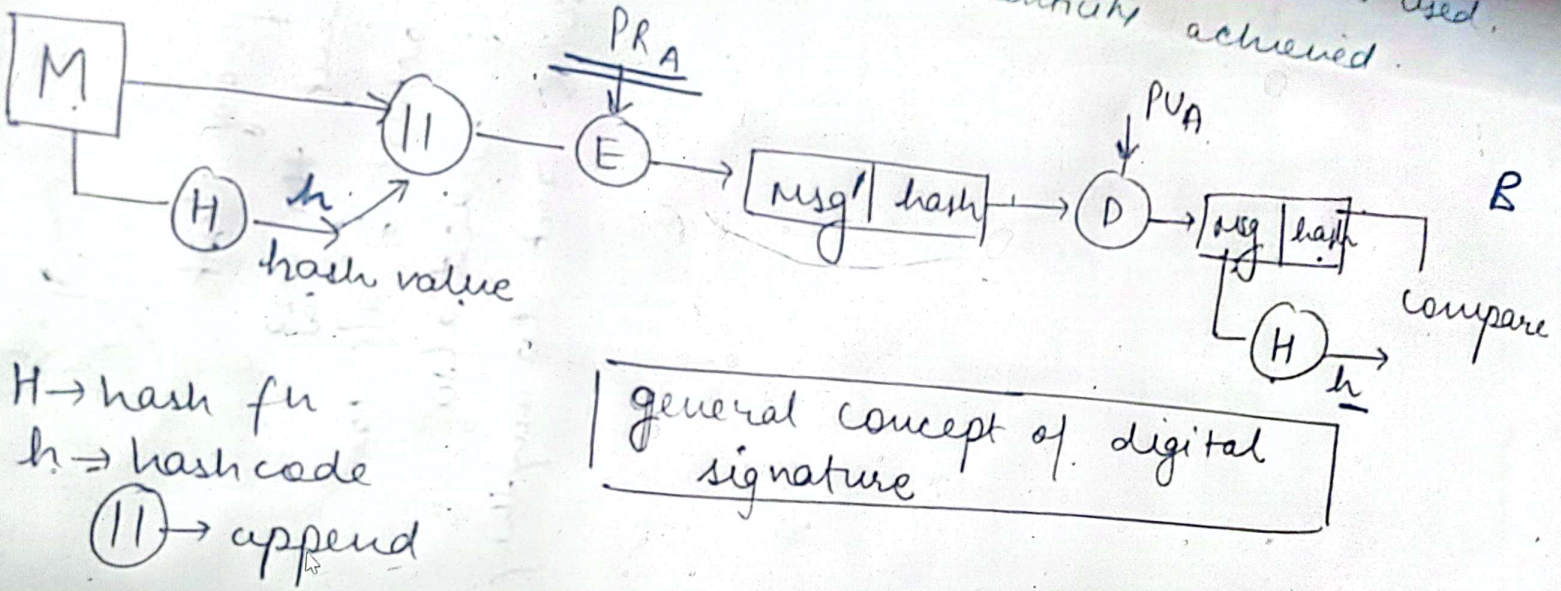
→ not used for confidentiality




→ also provides msg integrity

b/c if msg changed then at receiver

Digital signature




H → hash fn.
h → hash code
|| → append

∴ private key of Alice is used.
∴ authenticity achieved.

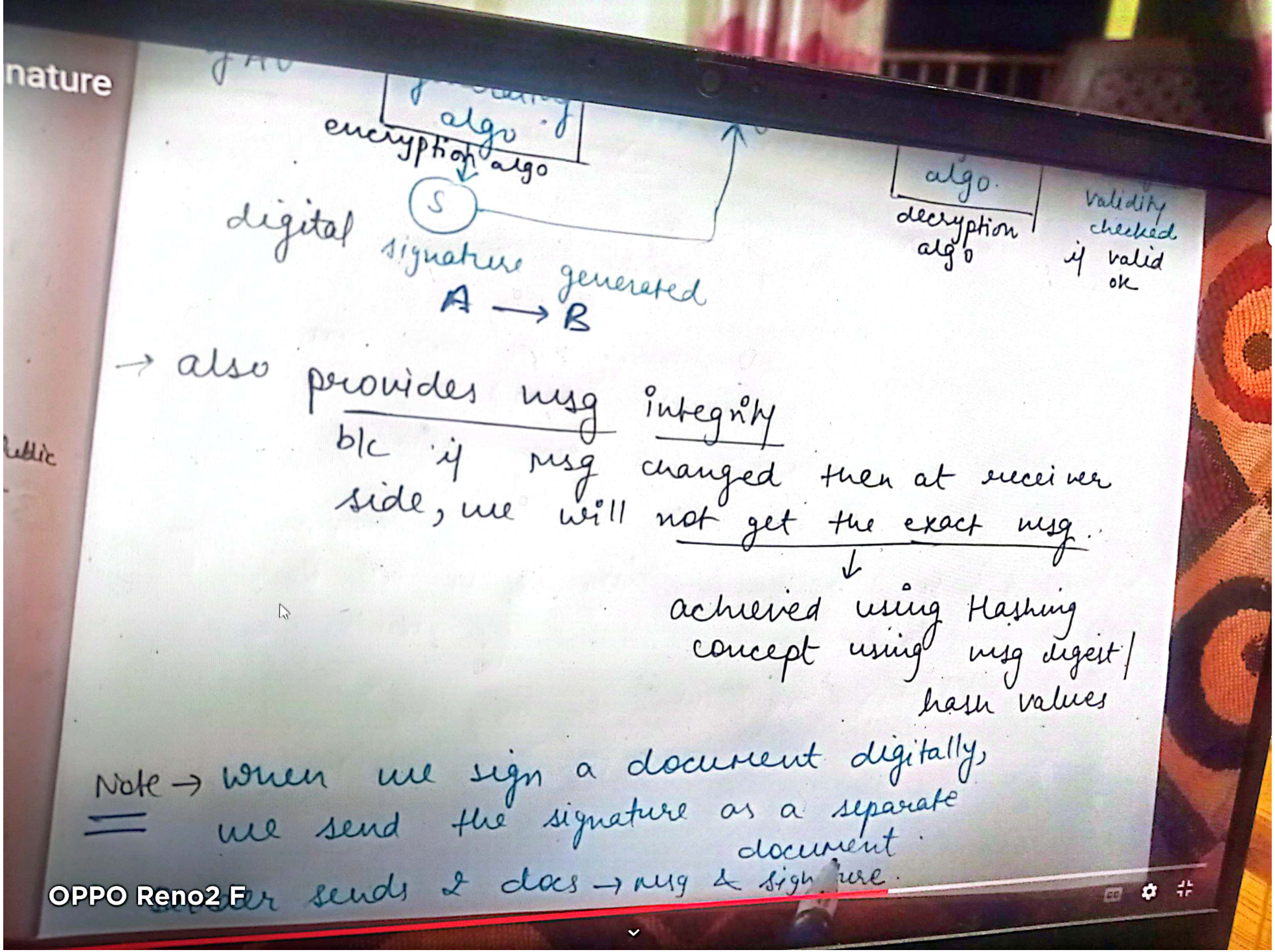
general concept of digital signature

Note → The signature must use some info. unique to the sender to prevent both forgery & denial.

Digital signature

7:36 / 12:53

OPPO Reno2 F



Digital signature

Non-repudiation
achieved by using a trusted 3rd party

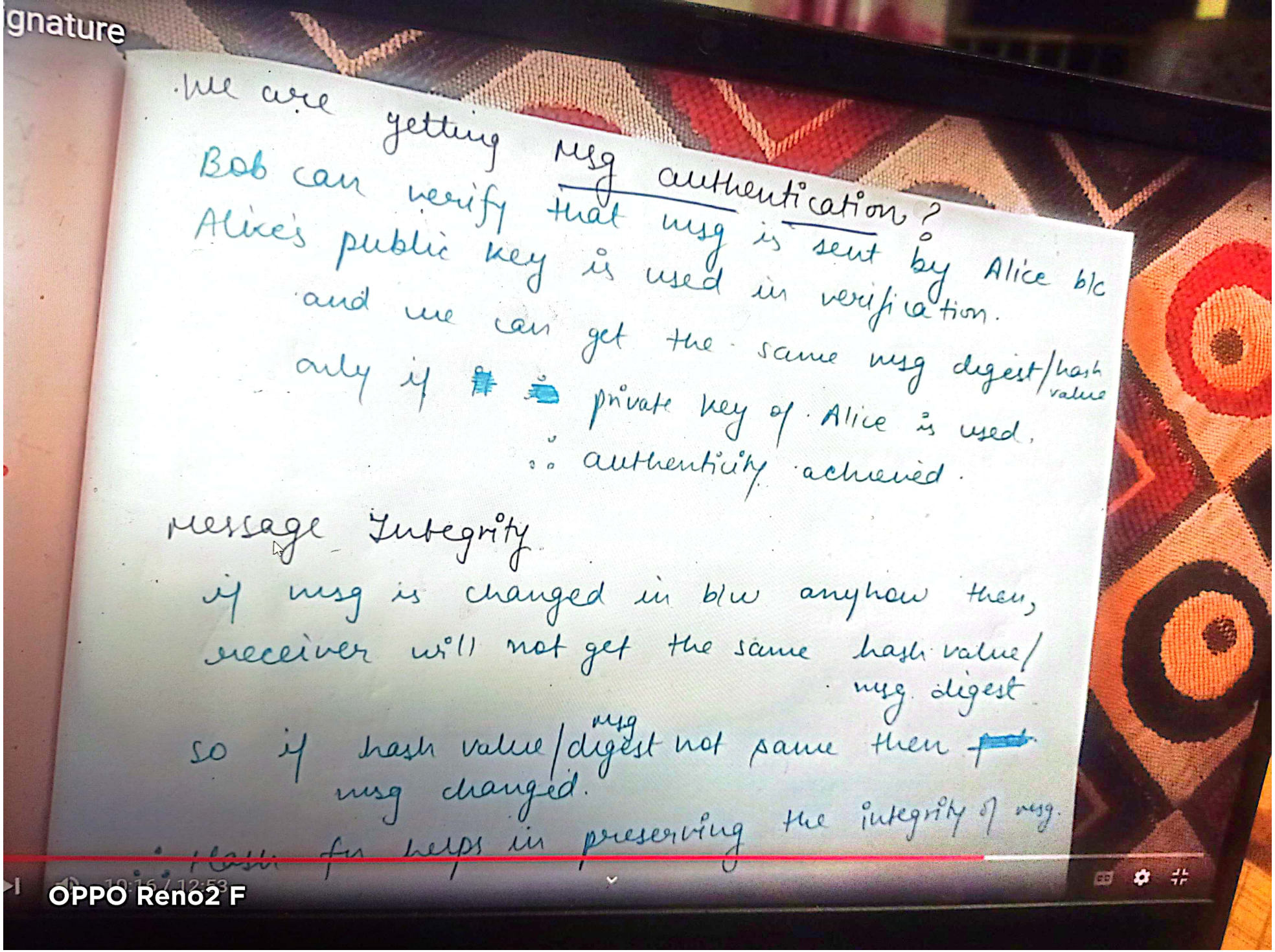
## Digital Signature

pg 351
pg 352

confidentiality

→ signature must use some info unique to the sender, to prevent forgery & denial.
→ It must be easy to produce digital signatures.
→ " " " " " to verify & recognize " " .
→ we need (i) key generation algo → to generate private key
(ii) Signing Algo i/p → M and Private key, o/p → Digital sign
(iii) verifying algo → using public key & sig

OPPO Reno2 F
9:46 / 12:53



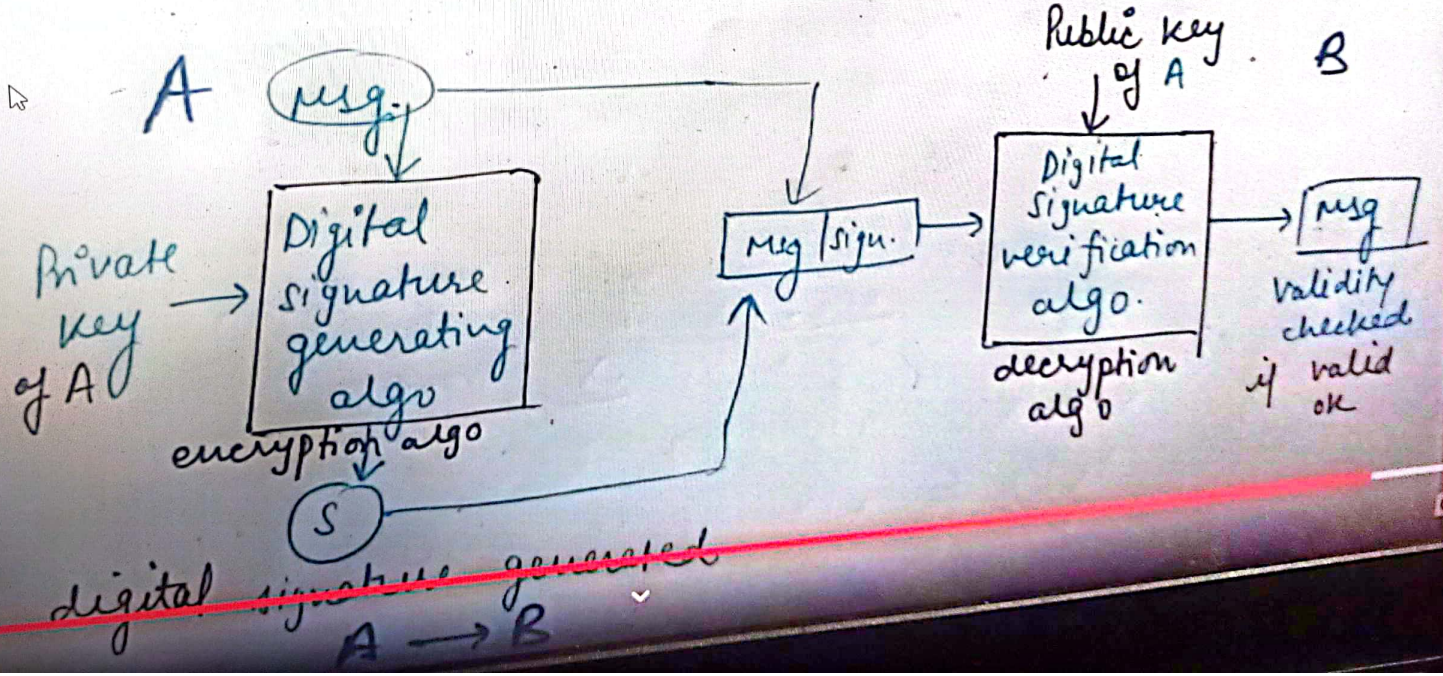
# Digital Signature

→ vimp role in e-commerce, online transaction, etc.

→ based on asymmetric key cryptography
encryption → private key
decryption → public key

→ used for msg authentication & non repudiation & msg integrity

→ not used for confidentiality



## 3.4 Confidentiality

A digital signature does not provide confidential communication. If confidentiality is required, the message and the signature must be encrypted using either a secret-key or public-key cryptosystem. Figure 13.5 shows how this extra level can be added to a simple digital signature scheme.

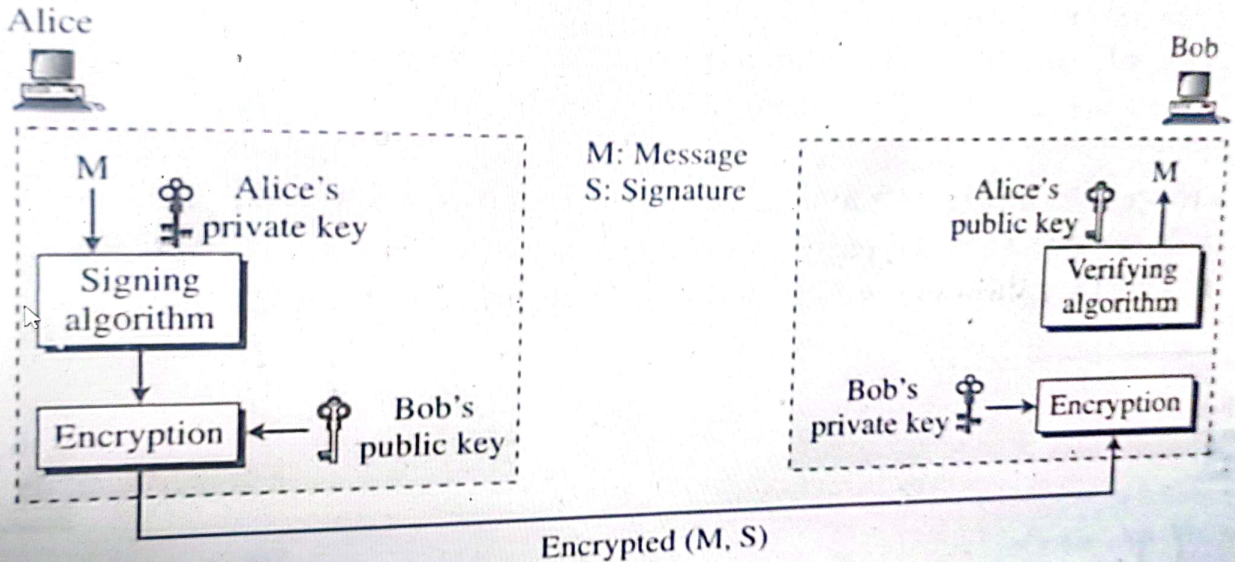



**Fig. 13.5** *Adding confidentiality to a digital signature scheme*

We have shown asymmetric-key encryption/decryption just to emphasize the type of keys used at each end. Encryption/decryption can also be done with a symmetric key.

Scheme using RSA concept

# RSA DIGITAL SIGNATURE SCHEME

→ The RSA idea can also be used to sign and verify a msg. In this case, it is called the RSA digital signature scheme.

→ The digital signature scheme changes the roles of the private and public keys

Note → 1st ly, the private & public keys of the sender are used (not of the receiver).

2nd → the sender uses his/her own private key to sign the document. and receiver uses the sender's public key to verify it.

OPPO Reno2 F

0:14 / 9:09

nature Scheme using RSA concept

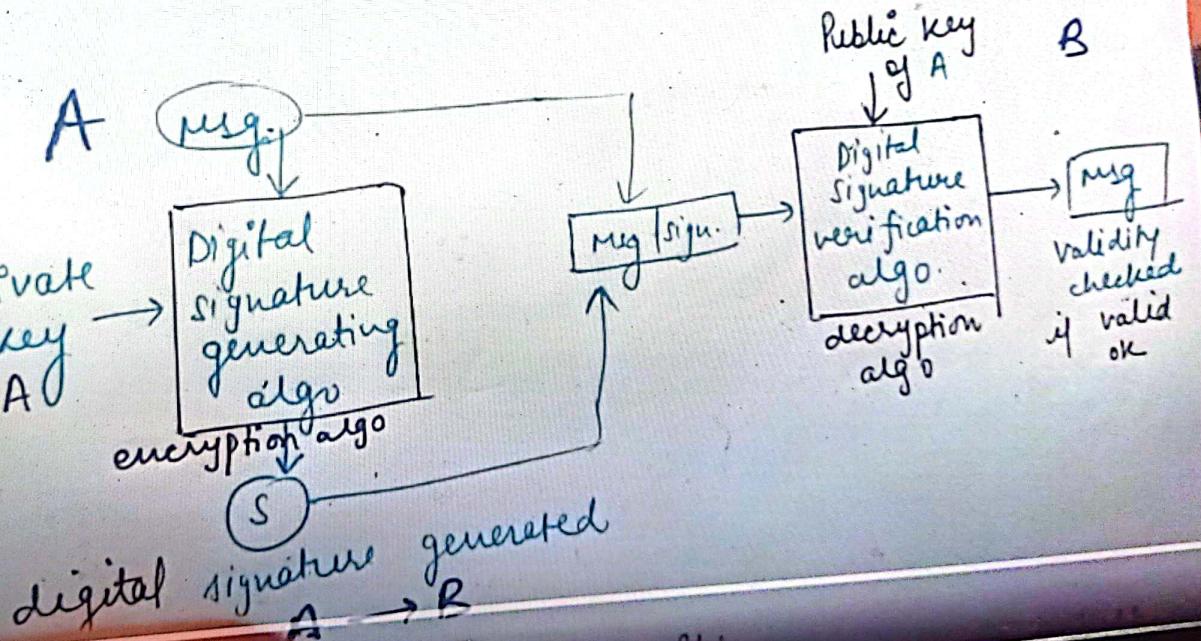
# Digital Signature

→ vimp role in e-commerce, online transaction, etc.

→ based on asymmetric key cryptography
encryption → private key
decryption → public key

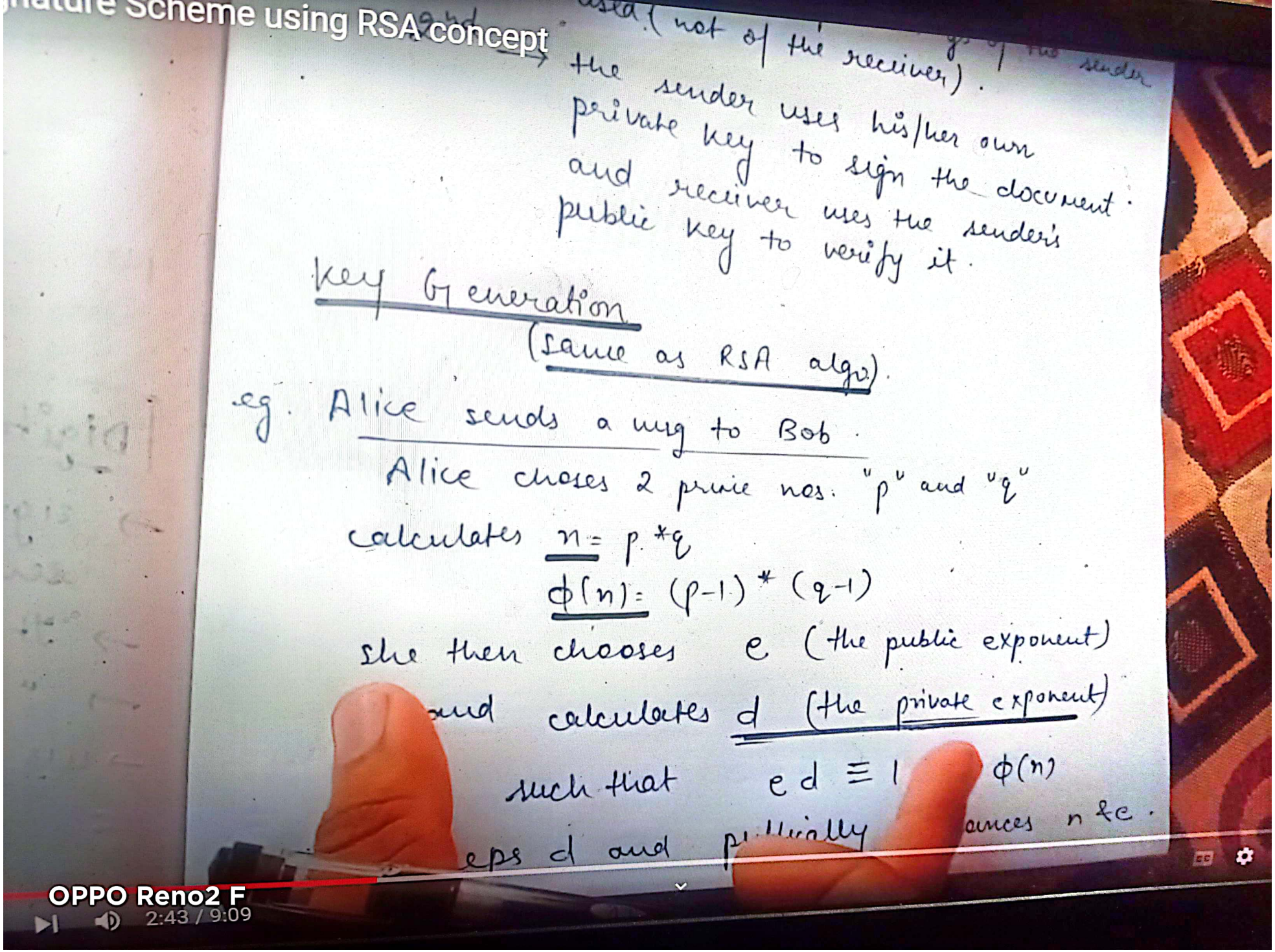
→ used for msg authentication & non repudiation & msg integrity

→ not used for confidentiality




OPPO Reno2 F

2:04 / 9:09



Scheme using RSA concept

A2A

In normal RSA,

Encryption

$C = M^e \bmod n$

$M < n$

$e, n$ → public key

Here,

for signing

$S = M^d \bmod n$

uses her private key
or we can say
she uses her private
exponent "d". to
create her signature.

Now, this signature "S" & message "M" is sent to Bob.

verifying → Bob receives "M" and "S"

Bob applies Alice's public exponent (e), to the signature to create a copy of message

$M' = S^e \bmod n$

OPPO Reno2 F

3:49 / 9:09

# Digital Signature Scheme using RSA concept



In the RSA digital signature scheme, $d$ is private; $e$ and $n$ are public.

## ❑ Signing and Verifying

Figure 13.7 shows the RSA digital signature scheme.

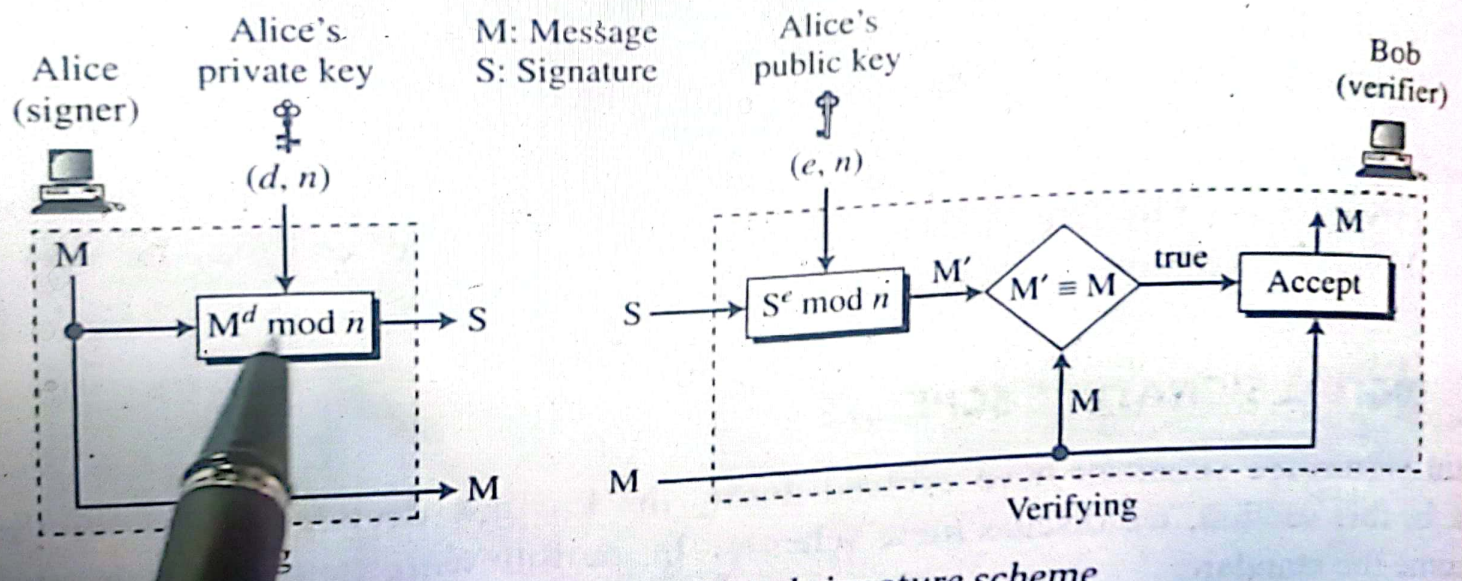



**Fig. 13.7** *RSA digital signature scheme*

a signature out of the message using her private exponent, $S = M^d \bmod n$ and

ture to Bob.

Bob applies Alice's public exponent to the signature to create a

Digital Signature Scheme using RSA concept

Here,

(n, e) → public key

for signing

$S = M^d \bmod n$

uses her private key
or we can say
she uses her private exponent "d". to create her signature.

"S" Signature & "M" is sent to Bob.

Cryptography and Network Security

tal signature scheme, d is private; e and n are public.

d Verifying

s the RSA digital signature scheme

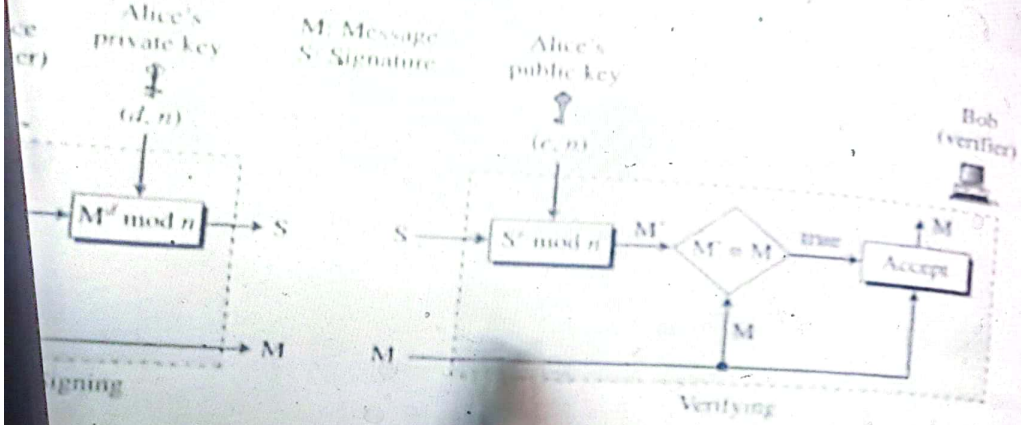



Fig. 13.7 RSA ... signature scheme

... a signature out of the ... ge using her private exponent, $S = M^d \bmod n$ and ... ature to Bob.

... es M and S. Bob appli... lice's public exponent to the signature to create a co... od n. Bob compare... alue of M' with the value of M. If the two values a... message. To prove ... e start with the verification criteria:

$M \pmod n \rightarrow \ldots \pmod n \rightarrow M^{d \times e} \equiv M \pmod n$

... because $d \times e = \ldots \pmod{\phi(n)}$ ... Euler's theorem in Chapter ...

→ Bob receives "M" and "S"

Bob applies Alice's public exponent (e), to the signature to create a copy of message $M' = S^e \bmod n$

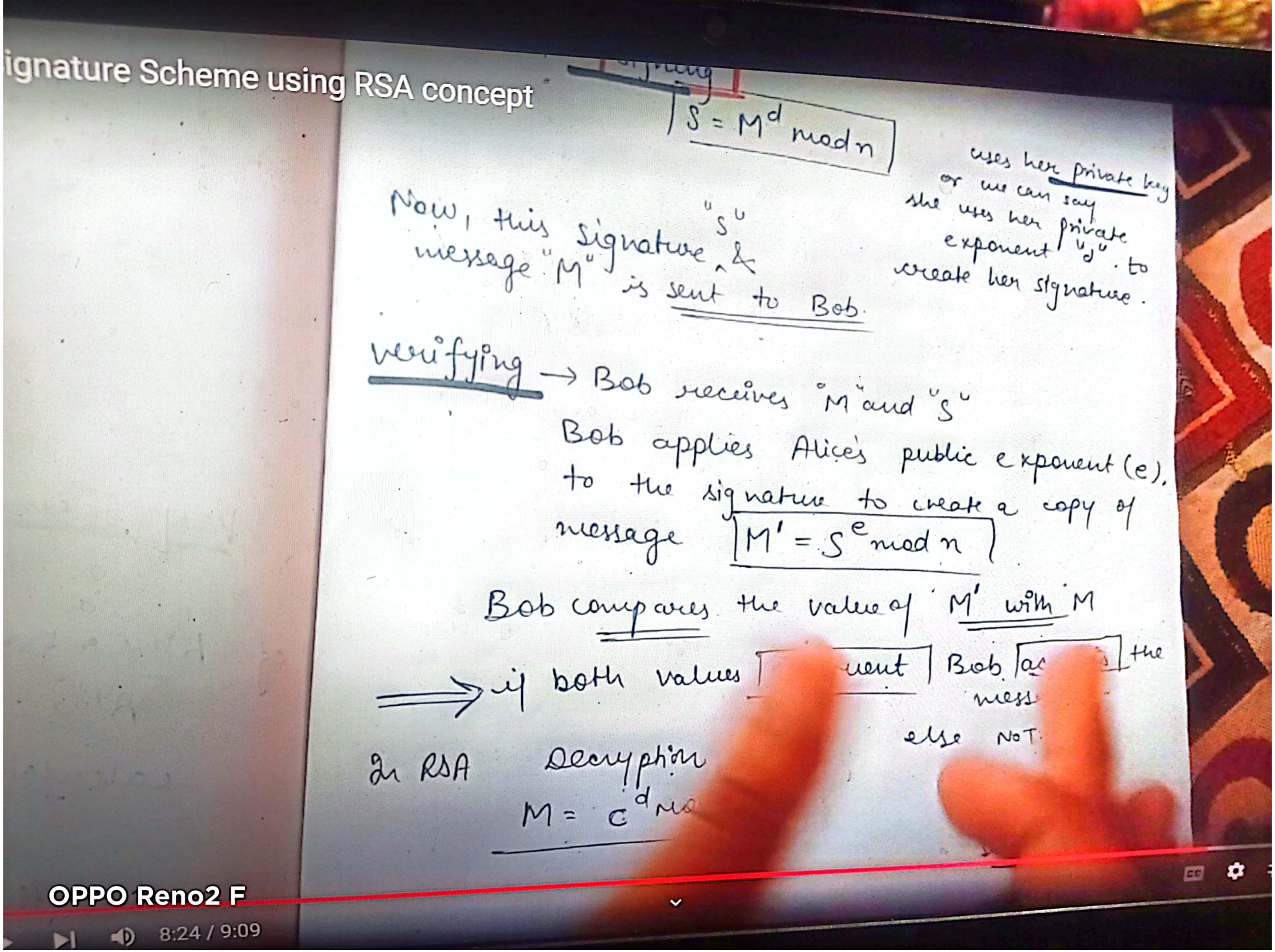
compares the value of M' with M

both values congruent Bob accepts the message

else NOT.

OPPO Reno2 F

7:06 / 9:09



In the RSA digital signature scheme, $d$ is private; $e$ and $n$ are public.

## Signing and Verifying

Figure 13.7 shows the RSA digital signature scheme.

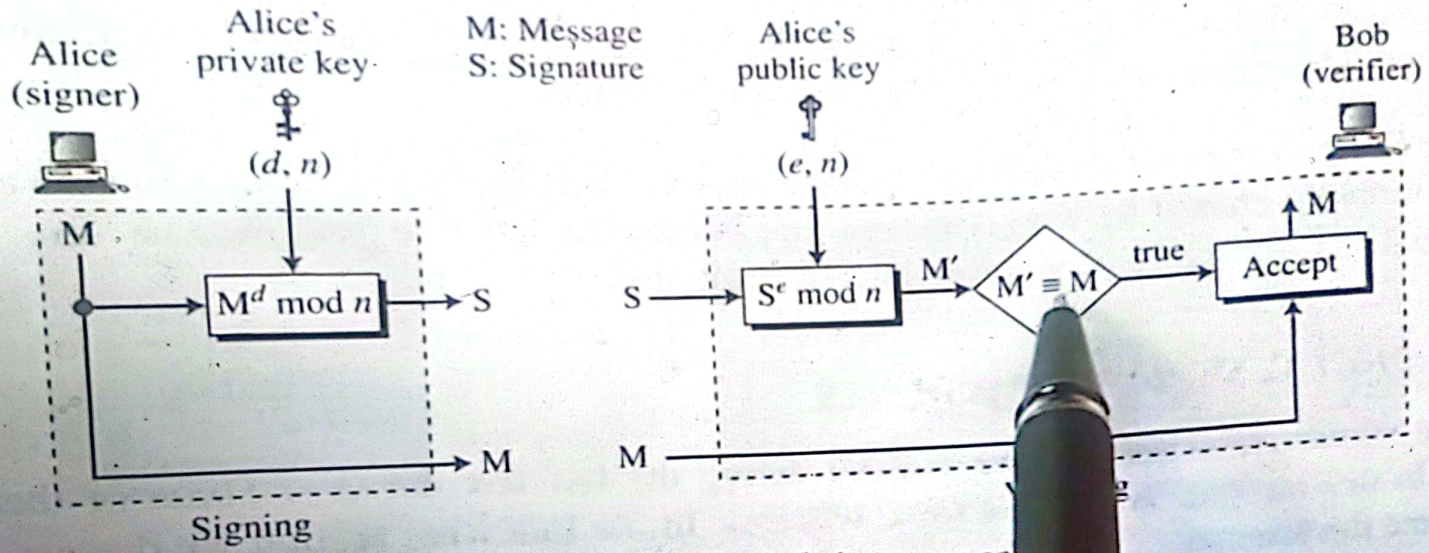



Fig. 13.7 *RSA digital signature sc*

**Signing** Alice creates a signature out of the message us… …nt, $S = M^d \bmod n$ and sends …ssage and the signature to Bob.

**Verifying** Bob … M and S. Bob applie…

# Elliptical Curve Cryptography

$$y^2 = x^3 + ax + b \pmod{11}$$

$$y^2 = x^3 + x + 6 \pmod{11}$$

$E_{11}(1,6)$

$a = 1,\ b = 6$

0 0 - - - - 10 $(\phi - 1)$

| $x$ | $x^3 + x + 6 \pmod{11}$ (RHS) |
|---|---|
| 0 | 6 |
| 1 | 8 |
| 2 | 5 |
| 3 | 2 |
| 4 | 8 |
| 5 | 4 |
| 6 | 8 |
| 7 | 4 |
| | 9 |
| | 7 |
| | 4 |

| $y$ | $y^2 \pmod{11}$ (LHS) |
|---|---|
| 0 | 0 |
| 1 | 1 |
| 2 | 4 |
| 3 | 9 |
| 4 | 5 |
| 5 | 3 |
| 6 | 3 |
| 7 | 5 |
| 8 | 9 |
| 9 | 4 |
| 10 | 1 |

(2,4) (2,7)

(3,5) (3,6)

(5,2) (5,9)

liptic Curve Cryptography |Encryption and Decryption |ECC in Cryptography & Security

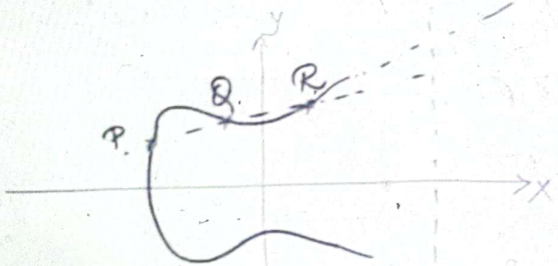
CTURES BY
LEDARSHAN

# Elliptic Curve Cryptography - Encryption & Decryption

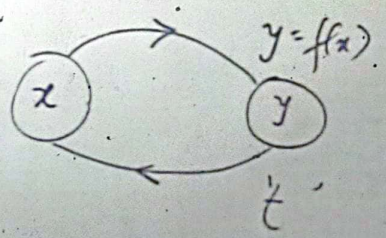
$y^2 = x^3 + ax + b$

asymetric, PKC.

| ECC (n) | RSA/DSA |
|---|---|
| 112 | 512 |
| 256 | 3072 |
| 512 | 15360 |

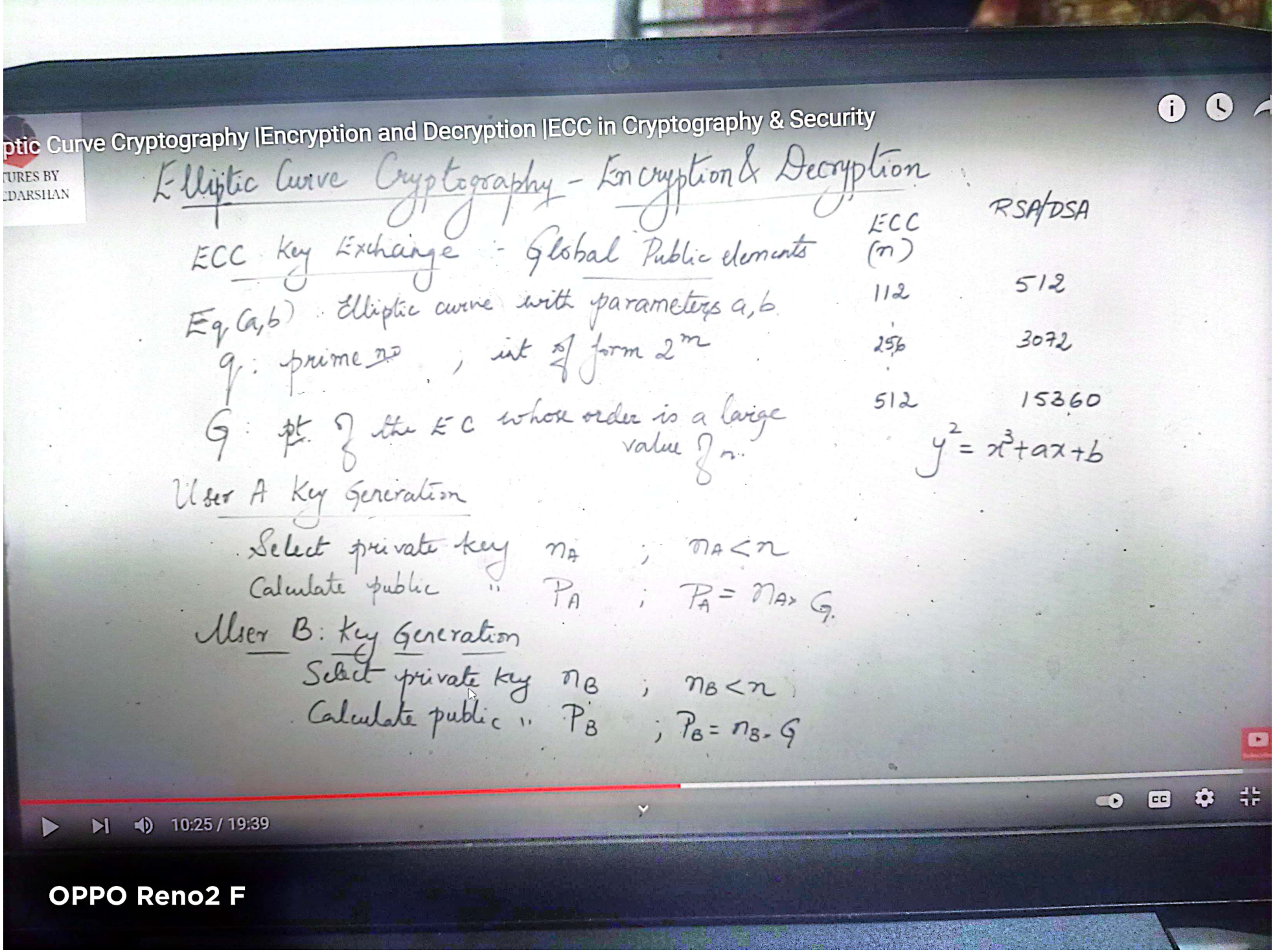



$E_p(a,b)$ ; $Q = kP$ $\quad k < n$ (limit)




6:20 / 19:39

OPPO Reno2 F



CS304: Introduction to Cryptography & Network Security

Assignment #1

Course Instructor: Dr. Dibyendu Roy Due: Feb 27, 2022, 11:59 pm

Instructions: Clearly write your name and roll number on the top of each page. Solutions must be written clearly. I expect all students to behave according to the highest ethical standards. Any cheating or dishonesty of any nature will result in deduction of marks.

**Problem 1**

Consider the plaintext (i.e., message) CRYPTOGRAPHY and the permutation $\pi$ on 12 numbers as defined below.

$$\pi : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 5 & 6 & 9 & 11 & 1 & 8 & 2 & 10 & 4 & 12 & 7 \end{pmatrix}$$

(a) Using the encryption technique of Transposition cipher encrypt the above plaintext.

(b) Check whether decryption is possible or not (provide justification). If decryption is possible write down the decryption technique.

**Problem 2**

Consider the plaintext (i.e., message) WEAREINDIAN and generate the ciphertext using the Shift cipher encryption algorithm with the secret key 4. Perform decryption on the ciphertext to check the correctness of your encryption.

**Problem 3**

Encrypt the plaintext WEAREINDIAN using Playfair cipher, where the secret key is CRICKET. Perform decryption on your generated ciphertext to validate your encryption.

**Problem 4**

In case of Affine cipher the key is $K = (a, b)$, where $0 \leq a, b \leq 25$ and the encryption algorithm is $y = Enc_K(x) = (a \cdot x + b) \mod 26$. Find out the case when the decryption is not possible. Write down the decryption algorithm when we can have successful decryption. Find out the exact number of different keys for which we will have the same plaintext-ciphertext pair $(x, y)$.

**Problem 5**

If $\mathsf{Enc}$ is the encryption function of DES then find out the relation between the ciphertexts $C_1 = \mathsf{Enc}(\mathsf{M}, \mathsf{K})$ and $C_2 = \mathsf{ENC}(\overline{\mathsf{M}}, \overline{\mathsf{K}})$. Here $\overline{X}$ denotes the bitwise complement of $X$ i.e., if $X = (x_1, \ldots, x_n)$ then $\overline{X} = (1 \oplus \overline{x_1}, \ldots, 1 \oplus \overline{x_n})$.

**Problem 6**

One unknown plaintext is encrypted using shift cipher encryption algorithm. The ciphertext is AFITIFWF. Find the plaintext and the secret key.

**Problem 7**

We use the following correspondence $A \to 0$, $B \to 1$, $\ldots$ , $Z \to 25$ to map english letters (A to Z) to numbers from 0 to 25. Let the message HILL is encrypted to XIYJ by using Hill cipher. Find atleast one possible key.

**Problem 8**

Using Euclidean algorithm solve the following problems.

(a) Find the $gcd(222, 18)$.

(b) Find $x_0, y_0$ such that $1 = 33x_0 + 13y_0$.

(c) If $b$ is the multiplicative inverse of $a$ under modulo $n$ i.e., $a \cdot b \equiv 1 \mod n$. Find the multiplicative inverse of 5 under modulo 26.

**Problem 9**

Prove that if we apply AES Subbytes function on $D3$ you will get 66 as output.

**Problem 10**

Find the AES-Mixcolumn$(33, 42, 66, 24)$. Here inputs and outputs are given in integer.

Jatin Goyal
2019510172

Q=1 message = CRYPTOGRAPHY

Permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 6 & 9 & 11 & 1 & 8 \end{pmatrix}$

$\begin{pmatrix} 8 & 9 & 10 & 11 & 12 \\ 2 & 10 & 4 & 12 & 7 \end{pmatrix}$

(a) In the encryption technique of transposition cipher what we do is we replace position of words in message.
Let the plain text is :-

$P_1 P_2 P_3 P_4 P_5 P_6 P_7 P_8 P_9 P_{10} P_{11} P_{12}$

we will replace it with :-

$P_3 P_5 P_6 P_9 P_{11} P_1 P_8 P_2 P_{10} P_4 P_{12} P_7$

So, the encryption of message CRYPTOGRAPHY will be YTOAHCRRPPYG

(b) To find the decryption of cipher text we will reverse permution $\pi$.

$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 8 & 1 & 10 & 2 & 3 & 12 & 7 & 4 & 9 & 5 & 11 \end{pmatrix}$

So, the decryption of YTOAHCRRPPYG will be CRYPTOGRAPHY

2019S1672
Jahn Goyal

Q=2 In the encryption of shift cipher we shift the character of plain text by K amount and if shift is more than 26 we take modulo.

Encryption = (Plain text + shift) mod 26

So, the encryption of message ~~we code~~ WEAREINDIAN will be :-

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Message → | W | E | A | R | E | I | N | D | I | A | N |
| Index → | 22 | 3 | 0 | 17 | 4 | 8 | 13 | 3 | 8 | 0 | 13 |
| Shift → | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| Adding → | 26 | 7 | 4 | 21 | 8 | 12 | 17 | 7 | 12 | 4 | 17 |
| taking mod → | 0 | 7 | 4 | 21 | 8 | 12 | 17 | 7 | 12 | 4 | 17 |
| Encrypted text | A | I | E | V | I | M | R | H | M | E | R |

Encrypted Text :- AIEVIMRHMER

Decryption = (cipher − shift + 26) mod 26

(A − 4 + 26) mod 26 = W
(I − 4 + 26) mod 26 = E
(E − 4 + 26) mod 26 = A
(V − 4 + 26) mod 26 = R
(I − 4 + 26) mod 26 = E
(M − 4 + 26) mod 21 = I
(R − 4 + 26) mod 26 = N
(H − 4 + 26) mod 26 = D
(M − 4 + 26) mod 26 = I
(E − 4 + 26) mod 26 = A

2019510072
Jatin Goyal

(R-4+26) mod 26 = N

so, decryption of AIEVIMRHMER will be WEAREINDIAN.

2019110172
Tatin Goyal

Q=3

Plain text = WEAREINDIAN
Secret Key = CRICKET

Encryption :-

First, we have to make a Key matrix

| | | | | |
|---|---|---|---|---|
| C | R | I | K | E |
| T | A | B | D | F |
| G | H | L | M | N |
| O | P | Q | S | U |
| V | W | X | Y | Z |

Second, we have to make pairs of plain text.

WE AR EI ND IA NX

WE :- As they are not in same row or same column so W → Z & E → R
= ZR

AR :- As they are in same column
so, A → H
R → A
AR = HA

EI :- They are in same row
so, E ⇒ C
I → K

2019510072
Jatin Goyal

EI = CK

ND :- As they are not in same row or same column.

So, N → M
D → F
ND = MF

IA :- They are also not in same row or column.

So, I → R
A → B
IA = RB

NX :- They are also not in same row or same column

So, N → L
X → 2
NX = L2

So, encryption of WEARE INDIAN is 2RHACKMFRBL2

2019116072
Jatin Goyal

Decryption :-
In decryption we will use same key matrix as encryption.

2R :- They are in different row and col.
2R = WE

HA :- They are in same column
HA = AR

CK :- They are in same row
CK = EI

MF :- They are in diff. row and col.
MF = ND

RB :- They are in diff. row & col.
RB = IA

LZ :- They are in diff. row & col.
LZ = NX

So, decryption of 2RHACKMFRBLZ will be WEAREINDIANX

2019S1072

Tatin Goyal

Q-4 Decryption of affine cipher is not possible if $a^{-1}$ does not exist. So, if (a, 26) are not coprime or hcf(a, 26) is not equal to 1 then $a^{-1}$ does not exist.

Decryption Algorithm :-

Decryption = ((c-b) * inv(a)) mod 26.

Let k be the inverse of a.

So, $k * a \% 26 = 1$

$k = inv(a) \bmod 26$

So, both (a, b) & (inv(a), b) will have the same ciphertext of a plaintext.

2019S1072
Jatin Goyal

Q-5

$C_1 = ENC(M, K)$
$C_2 = ENC(\bar{M}, \bar{K})$
$\bar{X}$ = bitwise complement of X
$X = (x_1, x_2 \cdots x_n)$

So by using the complement property of DES:

$ENC(M, K) = C$
$ENC(\bar{M}, \bar{K}) = \bar{C}$
$C_2 = ENC(\bar{M}, \bar{K})$
$\bar{C_2} = ENC(\bar{\bar{M}}, \bar{\bar{K}})$ $(\because \bar{\bar{X}} = X)$
$\bar{C_2} = ENC(M, K) = C_1$
$C_1 = \bar{C_2}$

Let $M = L_0 : R_0$
$L_1 = R_0$
$M = (R_0 \, XOR \, K)$ (round function)
$M = Sbox(m)$
$R_0 = L_0 \, XOR \, (m)$
$C_1 = L_1 : R_1$

Now $C_2 = ENC(\bar{M}, \bar{K})$
let $\bar{M} = \bar{L_0} : \bar{R_0}$
$L_1 = \bar{R_0} = \bar{R_0}$

2019S1672

Jatin Goyal

$M = (\overline{R_0} \text{ XOR } \overline{K})$

$M = (R_0 \text{ XOR } K)$ (XOR canal complement)

$M = (R_0 \text{ XOR } K)$ (same as round function)

$M = S60X(m)$

$R_1 = \overline{L_0} \text{ XOR } (m)$

$(R_1)_2 = \overline{R_1}$

$(L_1)_2 = \overline{L_1}$

$(C_1)_2 = (L_1)_2 (R_1)_2 = \overline{L_1}\,\overline{R_1} = \overline{C_1}$

$(C_1)_2 = \overline{C_1}$

Thus after a single round the ciphertext achevies is $(\overline{m}, \overline{K})$ is the complement of ciphertext $(m, K)$. Since, K is always complementary, this trend will happen in all rounds.

So, $C_2 = ENC(\overline{m}, \overline{K}) = \overline{C_1} = \overline{ENC}(m, K)$

Hence proved.

L0191692
Tahn Goyal

Q=6 ciphertext = AFITIFWF

encrypt → $(x + k) \bmod 26 = y$
decrypt → $(y - k) \bmod 26 = x$

F repeated 3 times.
$(5 - k) \bmod 26 = L$

$\frac{(L + k) \bmod 26}{(5 - k) \bmod 26} = \frac{5}{L}$

$(L + 5)(k + L - 5) = 0$
$\therefore L = 5 - k$

Now we will try for $k = 0, 1, 2, 3, 4, 5$
As most common word in english is 'A'. So, we will first try $k = 5$.
For $k = 5$
A → V, F → A, I → D, T → O
& W → R
So plaintext will be VADODARA.

2019516742

Jatin Goyal

Q=7

Message = HILL

Cipher = XIXJ

HILL = [7, 8, 11, 11]

XIXJ = [23, 8, 23, 9]

Let key = $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} K_1 & K_3 \\ K_2 & K_4 \end{bmatrix}$

Enc = $XK \pmod{26}$

Dec = $XK^{-1} \pmod{26}$

$[[7, 8][11, 11]] \begin{bmatrix} K_1 & K_3 \\ K_2 & K_4 \end{bmatrix} = \begin{bmatrix} 23 & 8 \\ 24 & 9 \end{bmatrix}$

$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} K_1 & K_3 \\ K_2 & K_4 \end{bmatrix} = \begin{bmatrix} 23 & 8 \\ 24 & 9 \end{bmatrix}$

$7K_1 + 8K_2 = 23$

$7K_3 + 8K_4 = 8$

$11K_1 + 11K_2 = 24$

$11K_3 + 11K_4 = 9$

on solving above equation

$K_1 = 11 \quad K_2 = 8 \quad K_3 = 3 \quad K_4 = 7$

$K = \begin{bmatrix} 11 & 3 \\ 8 & 7 \end{bmatrix}$ Ans

2019510912

Tahir Hoyal

Q=8 (a) gcd (222, 18)

Euclidean Theorem ⇒ $a = b*q + r$

If $A = 0$ then $gcd(A, B) = B$

$gcd(0, B) = B$

If $B = 0$ then $gcd(A, B) = A$

$gcd(A, 0) = A$

$222 = 18*12 + 6$

Here $r = 6$

$18 = 6*3 + 0$

Here $r = 0$

$gcd(222, 18) = 6$

(b) $1 = 33x_0 + 13y_0$

$33 = 13*2 + 7 \quad (r = 7)$

$13 = 7*1 + 6 \quad (r = 6)$

$7 = 6*1 + 1 \quad (r = 1)$

$6 = 1*6 + 0 \quad (r = 0)$

$1 = 7*6 - 1$

$1 = (33 - 13*2) - (13 - 7*1)$

$1 = (33 - 13*2) - 13 + (33 - 13*2)$

$1 = 2*33 - 5*13$

2619S1042

Tahir Goyal

after comparing

$1 = 2 * 33 - 5 * 13$

$1 = 33x_0 + 13y_0$

$x_0 = 2$

$y_0 = -5$

(c) $a \cdot b = 1 \bmod n$ ( b is mul. inv. of a)

$x = 5^{-1} \pmod{26}$

$5x = 1 \pmod{26}$

$5x = 105 \pmod{26}$

$5x = 21(5) \bmod 26$

$x = 21 \bmod 26$

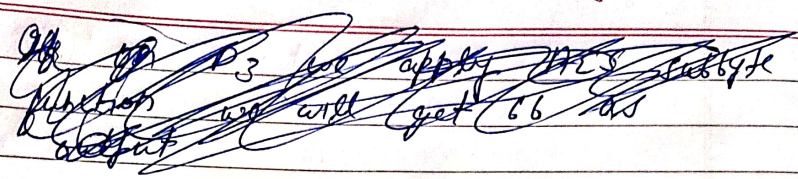
$x = 21$

2019S1072

John Loyal

classmate
Date
Page

Q=9



Q=10

2019S1072
Tahir Loyal

Q.10. AES mix column (33, 42, 66, 24)

$$\begin{bmatrix} K_1 \\ K_2 \\ K_3 \\ K_4 \end{bmatrix} = \begin{bmatrix} 33 \\ 42 \\ 66 \\ 24 \end{bmatrix}$$

$K_1 = 33 = 110011 = x^5+x^4+x+1$
$K_2 = 42 = 1000010 = x^6+x$
$K_3 = 66 = 1100110 = x^6+x^5+x^2+x$
$K_4 = 24 = 100100 = x^5+x^2$

$K_1' = x(K_1) + (x+1)K_2 + K_3 + K_4$
$= x^7 + x^6 + x^5 + x$
$= 11100010 = E2$

$K_2' = x(K_2) + (x+1)K_3 + K_4 + K_1$
$= x^7+x^2 + x^7+x^5 + x^3+x + x^5+x^2$
$+x^5+x^4 + x+1$
$= x^5+x^4 + x^3+1$
$= 00111001 = 39$

$K_3' = xK_3 + (x+1)K_4 + K_1 + K_2$
$= x^7 + x^6 + x^4 + 1$
$= 11010001$
$= D8$

2019S1072
Tahir Goyal

$$K_4' = xK_4 + (x+1)K_1 + K_2 + K_3$$
$$= x^5 + x^4 + 1$$
$$= 00110001$$
$$= 31$$

$$\begin{bmatrix} K_1 \\ K_2 \\ K_3 \\ K_4 \end{bmatrix} = \begin{bmatrix} E2 \\ 39 \\ D1 \\ 31 \end{bmatrix}$$

CS304: Introduction to Cryptography & Network Security

Assignment II

Course Instructor: Dr. Dibyendu Roy Due: Apr 22, 2022, 11:59 pm

Instructions: Clearly write your name and roll number on the top of each page. Solutions must be handwritten. I expect all students to behave according to the highest ethical standards. Any cheating or dishonesty of any nature will result in deduction of marks. Your submission will not be considered if you submit late.

---

**Problem 1** **2 marks**

The DES S-box $S_4$ has some unusual properties:

(a) Prove that the second row of $S_4$ can be obtained from the first row by means of the following mapping:

$$(y_1, y_2, y_3, y_4) \to (y_2, y_1, y_4, y_3) \oplus (0, 1, 1, 0)$$

where the entries are represented as binary strings.

(b) Show that any row of $S_4$ can be transformed into any other row by a similar type of operation.

**Problem 2** **1 mark**

Describe in detail how both encryption and decryption in CTR mode can be parallelized efficiently.

**Problem 3** **1 mark**

Suppose that $X = (x_1, \ldots, x_n)$ and $X' = (x'_1, \ldots, x'_n)$ are two sequences of $n$ plaintext blocks. Suppose $X$ and $X'$ are encrypted in OFB mode using the same key and the same IV. Show that it is easy for an adversary to compute $X \oplus X'$. Show that a similar result holds for CTR mode if ctr is reused.

**Problem 4** **1 mark**

Construct two LFSRs using the following two connection polynomials and find their periods.

(a) $f(x) = x^4 + x + 1$.

(b) $f(x) = x^5 + 1$.

**Problem 5** **1 mark**

Define a toy hash function $h : (\mathbb{Z}_2)^7 \to (\mathbb{Z}_2)^4$ by the rule $h(x) = xA$ where all operations are modulo 2 and the matrix $A$ is given below

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Find all preimages of $(0, 1, 0, 1)$.

**Problem 6** **1 mark**

Suppose $h_1 : \{0,1\}^{2m} \to \{0,1\}^m$ is a collision resistant hash function. Define $h_2 : \{0,1\}^{4m} \to \{0,1\}^m$ as follows:

(a) Write $x \in \{0,1\}^{4m}$ as $x = x_1 \parallel x_2$, where $x_1, x_2 \in \{0,1\}^{2m}$.

(b) Define $h_2(x) = h_1(h_1(x_1) \parallel h_1(x_2))$.

Show that $h_2$ is collision resistant.

**Problem 7** **1 mark**

Suppose $\lambda : \mathbb{Z}_{105} \to \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$ is defined as

$$\lambda(x) = (x \mod 3, x \mod 5, x \mod 7).$$

Give an explicit formula for the function $\lambda^{-1}$ and use it to compute $\lambda^{-1}(2, 2, 3)$.

**Problem 8** **1 mark**

Solve the following system of congruences:

$$\begin{aligned} x &\equiv 12 \mod 25 \\ x &\equiv 9 \mod 26 \\ x &\equiv 23 \mod 27. \end{aligned}$$

**Problem 9** **2 marks**

In RSA cryptosystem consider $n = 18923$ and the encryption key $e = 1261$. For the ciphertext $c = 6127$ find the corresponding plaintext. Explain each and every step.

**Problem 10** **2 marks**

Let $\mathsf{EL}$ be the elliptic curve $y^2 = x^3 + 5x + 3$ defined over $\mathbb{Z}_{13}$. Find out all the possible points on $\mathsf{EL}$. Provide justification against your answer.

Tatin Goyal
2019510172

Q=3. This problem can be solve easily by checking for every element in row 1 & apply operation and match with row 2.

| row 1 | Binary (row 1) $y_1 y_2 y_3 y_4$ | shift bits $(y_2, y_1, y_4, y_3)$ | XOR $(0,1,1,0)$ | Decimal |
|---|---|---|---|---|
| 7 | 0111 | 1011 | 1100 | 13 |
| 13 | 1101 | 1110 | 1000 | 8 |
| 14 | 1110 | 1101 | 1011 | 11 |
| 3 | 0011 | 0011 | 0101 | 5 |
| | | | | |
| 0 | 0000 | 0000 | 0110 | 6 |
| 6 | 0110 | 1001 | 1111 | 15 |
| 9 | 1001 | 0110 | 0000 | 0 |
| 10 | 1010 | 0101 | 0011 | 3 |
| | | | | |
| 1 | 0001 | 0010 | 0100 | 4 |
| 2 | 0010 | 0001 | 0111 | 7 |
| 8 | 1000 | 0100 | 0010 | 2 |
| 5 | 0101 | 1000 | 1100 | 12 |
| | | | | |
| 11 | 1011 | 0111 | 0001 | 1 |
| 12 | 1100 | 1100 | 1010 | 10 |
| 4 | 0100 | 1000 | 1110 | 14 |
| 15 | 1111 | 1111 | 1001 | 9 |

2019510072
Jatin Goyal

as we can see row: 1 & row 2. are same.

(b) By the above rule discussed we can show that 3rd row can be transformed into forth row.
To transform 1st row into 4th row.
(i) Convert entry into binary format $(y_1 y_2 y_3 y_4)$ where $y_i \in \{0,1\}$
(ii) compute $(y_4 y_3 y_2 y_1) \oplus (0,1,1,0)$

row $y_3$ can be transformed into $y_4$ using
$(y_1 y_2 y_3 y_4) \longrightarrow (y_2 y_1 y_4 y_3) \oplus (0,1,1,0)$

2019510072
Tatin Goyal

classmate
Date
Page

Q:2 Let length of plain text is m. In CTR mode we choose a counter denoted "ctr" which is bit string of length m.
we construct a sequence of bit string of length m denoted $T_1, T_2$ - - - defined as follows.

$$T_i = ctr + i - 1 \bmod 2^m$$

encrypt to plain text block $x_1, x_2, \ldots x_y$

$$y_i = x_i \oplus Enc(T_i)$$

as we can see that we can encrypt plaintext blocks independently of any other element.
So, we can parallely encrypt and decrypt blocks efficiently.

2019516072
Jatin Goyal

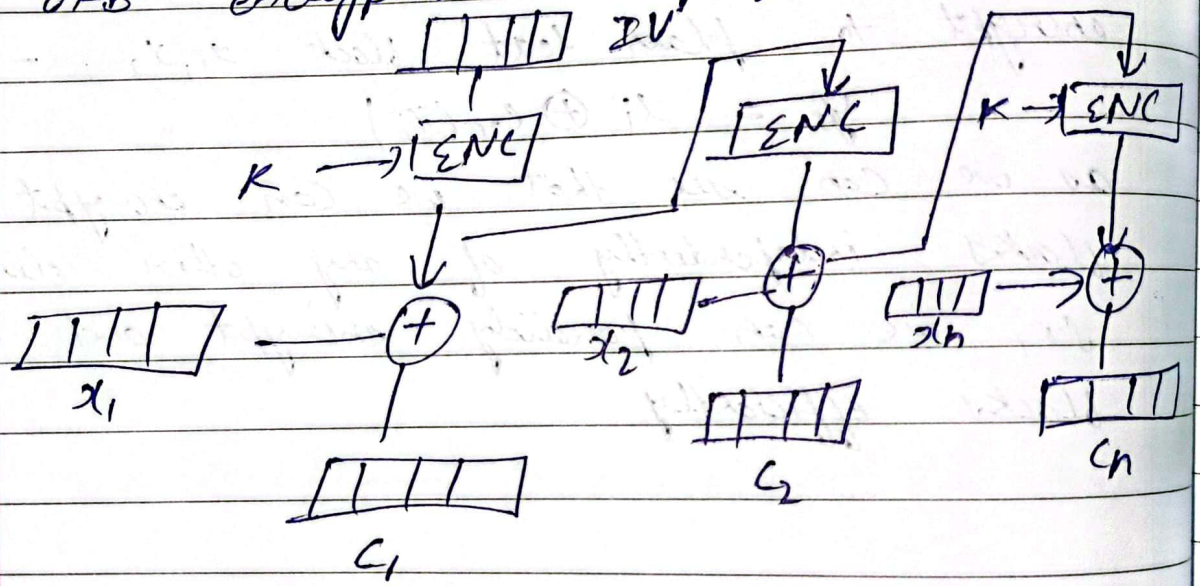
Q=3

h bit plaintext

$x = (x_1 \cdots x_h)$

$x' = (x_1' \cdots x_h')$

x & x' are encrypted in OFB mode using same key and the same IV. OFB encryption is performed.



2019516?2
Jatin Goyal



$n=4$ $\quad F(x) = x^4 + x + 1$

As we know from LFSR

$L(s) = C_1 s_{k-1} \oplus C_2 s_{k-2} - - - \oplus C_k s_0$

↑ feedback function

$F(x) = x^4 + x + 1$

$L = s_0 \oplus s_3$

| t | $s_3$ | $s_2$ | $s_1$ | $s_0$ |
|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 0 |
| 2 | 1 | 1 | 0 | 1 |
| 3 | 0 | 1 | 1 | 0 |
| 4 | 0 | 0 | 1 | 1 |
| 5 | 1 | 0 | 0 | 1 |
| 6 | 0 | 1 | 0 | 0 |
| 7 | 0 | 0 | 1 | 0 |
| 8 | 0 | 0 | 0 | 1 |
| 9 | 1 | 0 | 0 | 0 |
| 10 | 1 | 1 | 0 | 0 |
| 11 | 1 | 1 | 1 | 0 |
| 12 | 1 | 1 | 1 | 1 |
| 13 | 0 | 1 | 1 | 1 |
| 14 | 1 | 0 | 1 | 1 |
| 15 | 0 | 1 | 0 | 1 |

2019516 72
Jatin Goyal

output sequence =
101011 0010 0011 111
Period = 15 Ans

(b) $F(x) = x^5 + 1$

$L = 5_0$

| T | $S_4$ | $S_3$ | $S_2$ | $S_1$ | $S_0$ |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 |
| 2 | 0 | 1 | 0 | 1 | 1 |
| 3 | 1 | 0 | 1 | 0 | 1 |
| 4 | 1 | 1 | 0 | 1 | 0 |
| 5 | 0 | 1 | 1 | 0 | 1 |

output sequence
10110
Period = 5 Ans

2019510072
Jatin Goyal

Q-5

$h: (Z_2)^7 \rightarrow (Z_2)^4$

$h(a) = xA$

where $x$ is 7 bit length string

$h(x) \rightarrow$ 4 bit output

Let $x = [x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7]$

$h(x) = xA$

$$[x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7] \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} = [y_1\ y_2\ y_3\ y_4]$$

~~we need to find pre~~

we need to find pre image of [0 1 0 1]

find out all equation

$$x_1 + x_2 + x_3 + x_4 = 0 \quad - (i)$$
$$x_2 + x_3 + x_4 + x_5 = 1 \quad - (ii)$$
$$x_3 + x_4 + x_5 + x_6 = 0 \quad - (iii)$$
$$x_5 + x_5 + x_6 + x_7 = 1 \quad - (iv)$$

2019510742
Tatin Goyal

from eqn (i) & (iii)

$x_5 = 1 + x_1$

from (ii) & (iii)

$x_1 = 1 + x_2$

from (iii) & (iv)

$x_4 = 1 + x_3$

| $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_6$ | $x_7$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 1 | 1 | 1 | 0 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 1 | 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 |

2019510492
Tatin Goyal

Q=6 Let us assume there exists $x_1$ & $x_2$ such that $x_1 \neq x_2$ and

$h_2(x_1) = h_2(x_2)$

$x_1 = x_1' \,||\, x_2''$

$x_2 = x_2' \,||\, x_2''$

$x_1', x_2'' \in \{0,1\}^{2m}$

$x_2', x_2'' \in \{0,1\}^{2m}$

Since $h_2(x_1) = h_2(x_2)$

$h_2(x_1' \,||\, x_1'') = h_2(x_2' \,||\, x_2'')$

Since $h_2(x) = h_1(h_1(x) \,||\, h_1(x_2))$

$h_2(x_1) = h_1(h_1(x_1') \,||\, h_1(x_1''))$

$h_2(x_2) = h_1(h_1(x_2') \,||\, h_1(x_2''))$

Since, we assume

$h_2(x_1) = h_2(x_2)$

$h_1(h_1(x_1') \,||\, h_2(x_1'')) = h_1(h_1(x_2') \,||\, h_2(x_2''))$

$h_1(x_1') \,||\, h_1(x_1'') = h_1(x_2') \,||\, h_1(x_2'')$

If $h_1(x_1') = h_1(x_2')$

$h_1(x_1'') = h_1(x_2'')$

$x_1' = x_2'$, $x_1'' = x_2''$

So, it contradicts our assumption.

Therefore $h_2$ is collision resistant.

2019516772
Tatin Goyal

Q = 7

$\psi : 210 \rightarrow 2_3 \times 2_5 \times 2_7$

$\psi(x) = (x \bmod 3, x \bmod 5, x \bmod 7)$

$N = 105$

$N_1 = 35, \quad N_2 = 21, \quad N_3 = 15$

$35x_1 = 1 \bmod 3$

$x_1 = 2$

$21x_2 = 1 \bmod 5$

$x_2 = 1$

$15x_3 = 1 \bmod 7$

$x_3 = 1$

$\psi^{-1}(x) = (2 \times 35x_1 + 1 \times 21x_2 + 1 \times 15x_3) \bmod 105$

$\psi^{-1}(x) = (70x_1 + 21x_2 + 15x_3) \bmod 105$

$\psi^{-1}(2,2,3) = (70 \times 2 + 21 \times 2 + 15 \times 3) \bmod 105$

$= 227 \bmod 105$

$= 227 \bmod 105$

2019510172
Jatin Goyal

Q=8

$x \equiv 12 \mod 25$
$x \equiv 9 \mod 26$
$x \equiv 23 \mod 27$

$a_1 = 12 \quad m_1 = 25$
$a_2 = 9 \quad m_2 = 26$
$a_3 = 23 \quad m_3 = 27$

$M = m_1 \cdot m_2 \cdot m_3$
$= 17550$

$M_i = \frac{M}{m_i}$

$M_1 = \frac{17550}{m_1} = 702$

$M_2 = \frac{17550}{m_2} = 675$

$M_3 = \frac{17550}{m_3} = 650$

$M_1 M_1^{-1} = 1 \mod 25$
$702 (M_1^{-1}) = 1 \mod 25$
$M_1^{-1} = 13$

Tatin Goyal
20195107Q2



$M_2 \times M_2^{-1} = 1 \mod 26$

$M_2^{-1} = 25$

$M_3 M_3^{-1} = 1 \mod 27$

$650\ M_3^{-1} = 1 \mod 27$

$M_3^{-1} = 14$

$$X = \sum_{i=1}^{N} q_i M_i M_i^{-1}$$

$$= q_1 M_1 M_1^{-1} + q_2 M_2 M_2^{-1} + q_3 M_3 M_3^{-1}$$

$X = 109512 + 151875 + 209300$

$= 470687 \mod 17550$

~~$X = 14387$~~

$X = 14387$

Jatin Goyal
2019510072

Q=9 $n = 18923$ $e = 1261$ $C = 6127$

To decrypt the cipher text we will use the eqn $m = C^d \pmod{e}$

where d is decryption key which is obtained using p & q.

Here in the given question only n is given.

So for me there is not possible way to decrypt the ciphertext except for brute force method to find p & q from n.

Now to find d we will find p & q from n using brute force.

$n = 18923$

$p \& q = 127, 149$

Now to calculate $\phi(n)$

we know

$\phi(n) = (p-1)(q-1) \bmod n$

$= 18648$

Now for d : $de = 1 \bmod (18648)$

using extended euclidean

$d = 5797$

Now for plain text

$M = C^d \bmod n$

$M = 6127^{5797} \bmod 18923$

We will get plain text with it.

Tatik Goyal
2019510072



Q=10 Given $y^2 = x^3 + 5x + 3$

Hence $a = 5$, $b = 3$

where $x, y \in \{0, 1, \ldots, 12\}$

by brute force for every $x \in \{0, \ldots 12\}$ we find $y$.

| x/y | g $(x^3+5x+3) \bmod 13$ | g' $y^2 \bmod 13$ |
|---|---|---|
| 0 | 3 | 0 |
| 1 | 9 | 1 |
| 2 | 8 | 4 |
| 3 | 6 | 9 |
| 4 | 9 | 3 |
| 5 | 10 | 12 |
| 6 | 2 | 10 |
| 7 | 4 | 10 |
| 8 | 9 | 12 |
| 9 | 10 | 3 |
| 10 | 0 | 9 |
| 11 | 11 | 4 |
| 12 | 10 | 1 |

for points having on the curve g & g' must be equal.

Jatin Goyal
2019s1072



So, points on elliptic curve are as follow

(0, 4) (0, 9) (1, 3) (1, 10) (4, 3) (4, 10) (5, 6)
(5, 7) (7, 2) (7, 11) (8, 3) (8, 10) (9, 6)
(9, 7) (10, 0) (12, 6) (12, 7)

| | |
|---|---|
| **Started on** | Thursday, 10 March 2022, 2:30 PM |
| **State** | Finished |
| **Completed on** | Thursday, 10 March 2022, 3:49 PM |
| **Time taken** | 1 hour 18 mins |
| **Grade** | **24.00** out of 40.00 (**60**%) |

Question **1**

Correct

Mark 1.00 out of 1.00

Consider AES-128 in OFB mode of operation. One message $M$ of length 1024 bits has been encrypted using AES-128 in OFB mode of operation. During transmission 256-th bit and 512-th bit of the ciphertext are altered. Now the receiver performs the decryption on the received ciphertext and obtained the decrypted text $M'$.

Which of the following statement is true?

a. $M$ and $M'$ will differ at 256-th bit to 1024-th bit

b. $M$ and $M'$ will differ from 256-th bit to 512-th bit

c. $M$ and $M'$ will differ at 256-th bit and 512-th bit ✔

d. none of these

Your answer is correct.

The correct answer is:

$M$ and $M'$ will differ at 256-th bit and 512-th bit

Question **2**

Correct

Mark 1.00 out of 1.00

Let $C_1 = DES(M, K)$ and $C_2 = DES(\bar{M}, K)$. Which of the following relation is true?

a. $C_1 = C_2$

b. none of these ✔

c. $C_1 = \bar{C_2}$

Your answer is correct.

The correct answer is:

none of these

Question **3**

Incorrect

Mark 0.00 out of 1.00

Select the most appropriate one. Hash function has the following property

a. Finding preimage, collision, second preimage all are hard ✖

b. Preimage finding is hard

c. Second preimage finding is hard

d. Collision finding is hard

e. Finding preimage or collision or second preimage may not be hard

Your answer is incorrect.

The correct answer is:

Finding preimage or collision or second preimage may not be hard

Question **4**

Incorrect

Mark 0.00 out of 1.00

The expansion function of DES is

a. invertible

b. not invertible ✖

Your answer is incorrect.

The correct answer is:

invertible

Question **5**

Correct

Mark 1.00 out of 1.00

What is meant by the security of an Encryption Scheme?

a. An attacker who gets hold of a ciphertext should not be able to get any bit of the plaintext ✔

b. An attacker who gets hold of a ciphertext should not be able to get any function of the bits of the plaintext

c. An attacker who gets hold of a ciphertext should not be able to get the secret key used for the encryption

d. An attacker who gets hold of a ciphertext should not be able to know the plaintext

Your answer is correct.

The correct answer is:

An attacker who gets hold of a ciphertext should not be able to get any bit of the plaintext

Question **6**

Correct

Mark 1.00 out of 1.00

Assume that in a classroom there are 220 students. Form a group by

taking x many students randomly from the classroom. For which value

of x there will be atleast two students with same date of birth

with probability 0.7.

a. 30 ✔

b. 35

c. none of these

d. 28

Your answer is correct.

The correct answer is:

30

Question **7**

Correct

Mark 1.00 out of 1.00

Decryption of CBC mode of operation can be implemented in parallel

a. yes ✔

b. no

Your answer is correct.

The correct answer is:

yes

Question **8**

Correct

Mark 1.00 out of 1.00

The number of valid keys in the Affine Cipher over $\mathbb{Z}_{46}$ is

a. 2116

b. 46

c. none of these

d. 1012 ✔

Your answer is correct.

The correct answer is:

1012

Question **9**

Incorrect

Mark 0.00 out of 1.00

Select the correct answer where $S_1 : \{0,1\}^6 \rightarrow \{0,1\}^4$

and $S_2 : \{0,1\}^6 \rightarrow \{0,1\}^4$ are the pre-defined S-boxes

for the round function of DES.

a. $S_1(55) = 7$, $S_2(43) = 6$

b. $S_1(55) = 14$, $S_2(43) = 15$

c. $S_1(55) = 15$, $S_2(43) = 14$

d. none of these

e. $S_1(55) = 6$, $S_2(43) = 7$

Your answer is incorrect.

The correct answer is:

$S_1(55) = 14$, $S_2(43) = 15$

Question **10**

Correct

Mark 1.00 out of 1.00

If AES-Mixcolumn(23, 67, 45, 89) = (x,y,z,w) then y =

[here input and output are in integer]

a. 191 ✔

b. 229

c. 159

d. 121

Your answer is correct.

The correct answer is:

191

Question **11**

Correct

Mark 1.00 out of 1.00

Assume that in a classroom there are 250 students. Form a group by taking x many students randomly from the classroom. For which value of x there will be atleast two students with same date of birth with probability 0.9.

a. 30

b. 41 ✔

c. 35

d. none of these

Your answer is correct.

The correct answer is:

41

Question **12**

Correct

Mark 1.00 out of 1.00

For a fixed key any symmetric key encryption algorithm should

a. be surjective function

b. not necessary to be injective

c. be injective function ✔

d. not necessary to be surjective

e. none of these

Your answer is correct.

The correct answer is:

be injective function

Question **13**

Correct

Mark 1.00 out of 1.00

For each key DES is basically a permutation i.e., we can have $2^{56}$ such

permutations. With all these permutations consider the set G.

Now G with the operation composition of permutations

a. is not closed ✔

b. is closed

Your answer is correct.

The correct answer is:

is not closed

Question **14**

Incorrect

Mark 0.00 out of 1.00

Let $h : \mathbb{Z}_{2^{512}} \rightarrow \mathbb{Z}_{2^{256}}$ be a hash function

defined as $h(x) = (155x^4 + 201x^3 + 2x^2 + 101x + 1) \mod 2^{256}$ .

Is $h$ second preimage resistant?

a. yes ✖

b. no

Your answer is incorrect.

The correct answer is:

no

Question **15**

Correct

Mark 1.00 out of 1.00

If AES-Mixcolumn(23, 67, 89, 45) = (x,y,z,w) then w =

[here input and output are in integer]

a. 87

b. 145

c. 121 ✔

d. 159

e. none of these

Your answer is correct.

The correct answer is:

121

Question **16**

Correct

Mark 1.00 out of 1.00

SUBBYTES(6A) =

a. 24

b. 20

c. 34

d. none of these

e. 02 ✔

Your answer is correct.

The correct answer is:

02

Question **17**

Incorrect

Mark 0.00 out of 1.00

Let $F_k = F_{k-1} \oplus Enc(P_k, F_{k-1})$ be an iterated hash function where $Enc$ is the AES-128 encryption algorithm and $F_k, P_k$ each is of 128-bit. The initial $F_0$ is a 128-bit public data, $P_k$ is the $k$-th message block.

Which of the following statement is correct?

a. The above iterated hash function is a collision resistant hash function

b. The above iterated hash function is not a collision resistant hash function ✖

Your answer is incorrect.

The correct answer is:

The above iterated hash function is a collision resistant hash function

Question **18**

Correct

Mark 1.00 out of 1.00

Consider playfair cipher with the key KEYWORD. Which is the correct

ciphertext of the plaintext COMMUNICATION when the plaintext is

encrypted using playfair cipher with the mentioned key.

a. LCQTNTQGRBXFES ✔

b. LCQTNQTGRBXFES

c. LCQTNTQGBRXFES

d. none of these

e. LCQTNTQRGBXFES

Your answer is correct.

The correct answer is:

LCQTNTQGRBXFES

Question **19**

Correct

Mark 1.00 out of 1.00

Consider Affine cipher with the key K=(9, 19). Which is the correct

ciphertext of the plaintext INDIA when the plaintext is encrypted

using Affine cipher with the mentioned key.

a. NUGNT

b. NGTNU

c. NGUNM

d. none of these

e. NGUNT ✔

Your answer is correct.

The correct answer is:

NGUNT

Question **20**

Correct

Mark 1.00 out of 1.00

Consider Affine cipher with the key K=(11, 16). Which is the correct ciphertext

of the plaintext MIDSEM when the plaintext is encrypted using Affine cipher

with the mentioned key.

a. SAXIGS

b. none of these

c. SAXGSI

d. SAGXIS

e. SAXGIS ✔

Your answer is correct.

The correct answer is:

SAXGIS

Question **21**

Incorrect

Mark 0.00 out of 1.00

Consider one round of Feistel network with the block size 64-bit and

the secret key K of size 32-bit. The round function is defined by

$f(R_0, K) = S(R_0 \oplus K)$ where $S(X) = (X + 1) \mod 2^{32}$.

Find the ciphertext for the plaintext = 1 and key K = 1.

a. 2147483648

b. 2147483649 ✖

c. 4294967297

d. 4294967296

e. none of these

Your answer is incorrect.

The correct answer is:

4294967297

Question **22**

Incorrect

Mark 0.00 out of 1.00

Let $P$, $C$, $K$ be the plaintext space, ciphertext space and key space respectively.

Consider an encryption algorithm $E$ with the following conditions:

1. $|P| = |C| = |K|$

2. every key is equiprobable

3. for every $p \in P$, $c \in C$ there is an unique key $k$ such that $E(p,k) = c$,

Select the most appropriate option

a. $E$ will provide perfect secrecy if $|K| > |P|$

b. $E$ provides perfect secrecy

c. $E$ can not provide perfect secrecy as it differs from OTP ✖

Your answer is incorrect.

The correct answer is:

$E$ provides perfect secrecy

Question **23**

Correct

Mark 1.00 out of 1.00

Encryption of CBC mode of operation can be implemented in parallel

a. no ✔

b. yes

Your answer is correct.

The correct answer is:

no

Question **24**

Correct

Mark 1.00 out of 1.00

Let $F$ denotes the AES-128 bit encryption algorithm.

Define a function $f:\{0,1\}^{128} \rightarrow \{0,1\}^{128}$ as

$f(x) = F(x,K) \oplus x$ , here $x, K$ are of 128-bits and $K$ is a fixed secret key.

Which of the following statement is correct?

a. $f$ is not an one-way function

b. $f$ is an one-way function ✔

Your answer is correct.

The correct answer is:

$f$ is an one-way function

Question **25**

Correct

Mark 1.00 out of 1.00

S-boxes in DES map

a. 2 bits to 4 bits

b. 4 bits to 6 bits

c. none of these

d. 4 bits to 4 bits

e. 6 bits to 4 bits ✔

Your answer is correct.

The correct answer is:

6 bits to 4 bits

Question **26**

Correct

Mark 1.00 out of 1.00

Expanded key size of AES-256 is

a. 56 words

b. 44 words

c. 60 words ✔

d. none of these

e. 48 words

Your answer is correct.

The correct answer is:

60 words

Question **27**

Correct

Mark 1.00 out of 1.00

Let $h:\{0,1\}^* \to \{0,1\}^n$ be a preimage resistant and collision resistant

hash function. Define a new hash function $h':\{0,1\}^* \to \{0,1\}^{n+1}$

by using following rule $h'(x) = 0||x$ if $x \in \{0,1\}^n$ ,

otherwise $h'(x) = 1||h(x)$ . Which of the following statement is true.

a. $h'$ is neither preimage resistant nor collision resistant

b. $h'$ is not a preimage resistant but collision resistant ✔

c. $h'$ is a preimage resistant as well as collision resistant

Your answer is correct.

The correct answer is:

$h'$ is not a preimage resistant but collision resistant

Question **28**

Incorrect

Mark 0.00 out of 1.00

What are the correct values of x,y such that 23x+43y=gcd(23,43)?

a. none of these

b. x=-24,y=16

c. x=25,y=-18

d. x=13,y=7 ✖

e. x=15,y=-8

Your answer is incorrect.

The correct answer is:

x=15,y=-8

Question **29**

Incorrect

Mark 0.00 out of 1.00

Which is the multiplicative inverse of $(x^4+x^3+x+1)$ in $(\mathbb{F}_2[x]/<x^8+x^4+x^3+x+1>,+,*)$ .

Here + and * are the polynomial addition and polynomial multiplication under modulo $x^8+x^4+x^3+x+1$.

a. $x^7+x^6+x^3+x^2$

b. $x^7+x^6+x^3+x^2+1$ ✖

c. $x^7+x^6+x^2+x+1$

d. $x^7+x^6+x^5+1$

e. none of these

Your answer is incorrect.

The correct answer is:

$x^7+x^6+x^3+x^2$

Question **30**

Incorrect

Mark 0.00 out of 1.00

Consider one-bit encryption $C = P \oplus K$. If $Pr[K = 0] = 0.5$ and $Pr[P = 1] = 0.3$

then $Pr[P = 0|C = 1]$ is

a. none of these

b. 0.4

c. 0.7

d. 0.5

e. 0.3 ✖

Your answer is incorrect.

The correct answer is:

0.7

Question **31**

Incorrect

Mark 0.00 out of 1.00

A sequence of plaintext blocks x1,...,xn are encrypted by

using AES-128 in CBC mode. The corresponding ciphertext blocks

are y1,...,yn. During transmission y1 is transmitted incorrectly

(i.e., some 1's are changed to 0's and vice verse).

The number of plaintext blocks that will be decrypted incorrectly is

a. 3

b. 2

c. n

d. none of these

e. 1 ✖

Your answer is incorrect.

The correct answer is:

2

Question **32**

Incorrect

Mark 0.00 out of 1.00

Consider AES-128 in CFB mode of operation. One message of length 1024 bits

has been encrypted using AES-128 in CFB mode of operation.

Now to decrypt the ciphertext which of the following process needs to be followed

a. decryption of AES-128 needs to fit in CFB mode ✖

b. encryption of AES-128 needs to fit in CFB mode

Your answer is incorrect.

The correct answer is:

encryption of AES-128 needs to fit in CFB mode

Question **33**

Incorrect

Mark 0.00 out of 1.00

Consider AES-128 in OFB mode of operation. One message of length 1024 bits

has been encrypted using AES-128 in OFB mode of operation. Now to decrypt the

ciphertext which of the following process needs to be followed

a. decryption of AES-128 needs to fit in OFB mode ✖

b. encryption of AES-128 needs to fit in OFB mode

Your answer is incorrect.

The correct answer is:

encryption of AES-128 needs to fit in OFB mode

Question **34**

Correct

Mark 1.00 out of 1.00

Consider playfair cipher with the key MIDSEM. Which is the correct

ciphertext of the plaintext VADODARA when the plaintext is

encrypted using playfair cipher with the mentioned key.

a. none of these

b. MHELMCPC ✔

c. MHLEMCPC

d. MHEMLCPC

e. MHELCMPC

Your answer is correct.

The correct answer is:

MHELMCPC

Question **35**

Correct

Mark 1.00 out of 1.00

Let $n = p \times q$ where $p, q$ are two large primes.

Here $n$ is known to everyone and $p, q$ are hidden.

Consider the hash function $h(x) = x^2 \mod n$.

a. $h$ is an one-way function ✔

b. $h$ is not an one-way function

Your answer is correct.

The correct answer is:

$h$ is an one-way function

Question **36**

Incorrect

Mark 0.00 out of 1.00

How many distinct predefined functions are used in SHA-1

a. none of these

b. 3

c. 4

d. 80 ✖

Your answer is incorrect.

The correct answer is:

3

Question **37**

Correct

Mark 1.00 out of 1.00

If all the 16 round keys of DES are identical then

a. DES encryption and decryption functions will not be identical due to the IP

b. DES encryption and decryption functions will be exactly equal ✔

c. none of these

d. only the last round and first round of DES will be identical

Your answer is correct.

The correct answer is:

DES encryption and decryption functions will be exactly equal

Question **38**

Incorrect

Mark 0.00 out of 1.00

Which of the following statement is correct?

a. if encryption function is oneway then decryption is not possible

b. encryption function is oneway if the private key is unknown

c. only hash functions are oneway functions ✖

Your answer is incorrect.

The correct answer is:

encryption function is oneway if the private key is unknown

Question **39**

Incorrect

Mark 0.00 out of 1.00

Which is the multiplicative inverse of $(x^3+x^2+1)$ in

$(\mathbb{F}_2[x]/<x^8+x^4+x^3+x+1>,+,*)$ . Here + and * are

the polynomial addition and polynomial multiplication under

modulo $x^8+x^4+x^3+x+1$.

a. $x^7+x^6+x^3+x^2$

b. none of these

c. $x^7+x^6+x+1$ ✖

d. $x^7+x^6+x^5+1$

e. $x^7+x^6+x^2+1$

Your answer is incorrect.

The correct answer is:

$x^7+x^6+x^5+1$

Question **40**

Correct

Mark 1.00 out of 1.00

Let $h : \mathbb{Z}_{512} \times Z_{512} \rightarrow \mathbb{Z}_{512}$ be a hash

function defined as $h(x, y) = (ax + by) \mod 512$, $a, b \in \mathbb{Z}_{512}$.

Which of the following is correct?

a. $h$ is not an ideal hash function ✔

b. $h$ is an ideal hash function

Your answer is correct.

The correct answer is:

$h$ is not an ideal hash function

◄ Announcements

Jump to...