THE HASH GAME

THE FOSS FILES SEASON 5 | EPISODE 1

THE CIPHER FILES

Ameya Unchgaonkar

Bhakti More

Aditya Aparadh

WLUG
COMMUNITY | KNOWLEDGE | SHARE

TABLE OF CONTENT

WLUG
COMMUNITY | KNOWLEDGE | SHARE

INTRODUCTION TO CRYPTOGRAPHY

INTRODUCTION TO CRYPTOGRAPHY

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Cryptography is the science of securing information and communications so that only the intended recipient can access and understand it

WLUG

COMMUNITY | KNOWLEDGE | SHARE

A B C D E F G H I J K L M N

O P Q R S T U V W X Y Z

WLUG

COMMUNITY | KNOWLEDGE | SHARE

A B C

D E F

WLUG
COMMUNITY | KNOWLEDGE | SHARE

A

D

Shift by 3

B

E

Shift by 3

C

F

WLUG
COMMUNITY | KNOWLEDGE | SHARE

CAESAR CIPHER

A → D (Shift by 3)

B → E (Shift by 3)

C → F

WLUG
COMMUNITY | KNOWLEDGE | SHARE

CAESAR CIPHER

? ? ? ?

Z O X J

WLUG
COMMUNITY | KNOWLEDGE | SHARE

CAESAR CIPHER

W L U G

Z O X J

WLUG
COMMUNITY | KNOWLEDGE | SHARE

PLAIN TEXT AND CIPHERTEXT

WLUG

ZOXJ

Plain Text

Cipher Text

WLUG
COMMUNITY | KNOWLEDGE | SHARE

THE NEED OF CRYPTOGRAPHY

WLUG
COMMUNITY | KNOWLEDGE | SHARE

THE NEED OF CRYPTOGRAPHY

Integrity: Detect and prevent unauthorized alterations

Confidentiality: Ensure data is accessible only to authorized parties

WLUG
COMMUNITY | KNOWLEDGE | SHARE

THE NEED OF CRYPTOGRAPHY

Integrity: Detect and prevent unauthorized alterations

Confidentiality: Ensure data is accessible only to authorized parties

WLUG
COMMUNITY | KNOWLEDGE | SHARE

THE NEED OF CRYPTOGRAPHY

Authentication: Verify the identity of participants in a communication

Non-repudiation: Ensure a sender cannot deny the authenticity of their message

WLUG
COMMUNITY | KNOWLEDGE | SHARE

HISTORY

ENIGMA MACHINE

The Enigma machine was a cipher device used by the German military to encrypt and decrypt messages during World War II

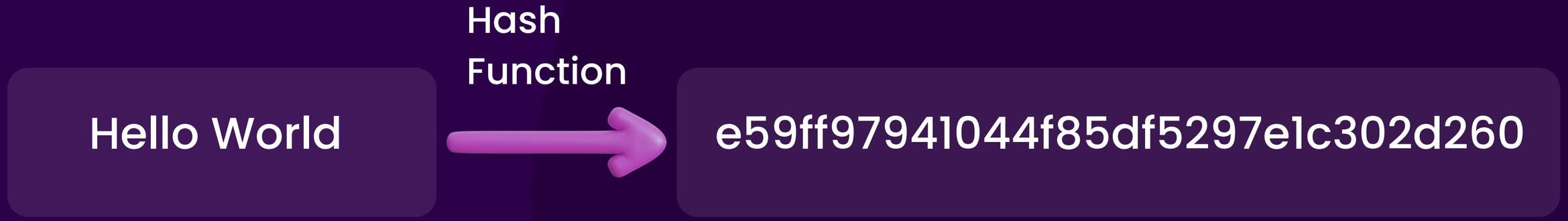
WLUG
COMMUNITY | KNOWLEDGE | SHARE

INTRODUCTION TO HASHING

Hashing is the process of transforming any given key or a string of characters into another value.

WLUG
COMMUNITY | KNOWLEDGE | SHARE

INTRODUCTION TO HASHING



WLUG
COMMUNITY | KNOWLEDGE | SHARE

Hello World

WLUG

COMMUNITY | KNOWLEDGE | SHARE

Hello World

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Hello World

Hello World

WLUG

COMMUNITY | KNOWLEDGE | SHARE

Hello World

Hello World

WLUG
COMMUNITY | KNOWLEDGE | SHARE

CHECKSUM

Hello World

H = 72, e = 101, l = 108, l = 108, o = 111, (space) = 32,
W = 87, o = 111, r = 114, l = 108, d = 100

WLUG
COMMUNITY | KNOWLEDGE | SHARE

CHECKSUM

Hello World

Hello World = 1052

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Hello World

1052

WLUG

COMMUNITY | KNOWLEDGE | SHARE

Hello World

1052

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Hello World = 1052

1052

WLUG
COMMUNITY | KNOWLEDGE | SHARE

HASHING

Hello World

B10A8DB164
E0754105B7A
99BE72E3FE5

Hash Function

(md5 , sha , argon2)

WLUG
COMMUNITY | KNOWLEDGE | SHARE

DETERMINISM

Hello World

Hash Function

(md5 , sha , argon2)

B10A8DB164
E0754105B7A
99BE72E3FE5

Same Input >>> Same output

WLUG
COMMUNITY | KNOWLEDGE | SHARE

FIXED-LENGTH OUTPUT

Hello
World

B10A8DB164
E0754105B7A
99BE72E3FE5

Variable length

Hash Function
(md5 , sha , argon2)

Fixed length

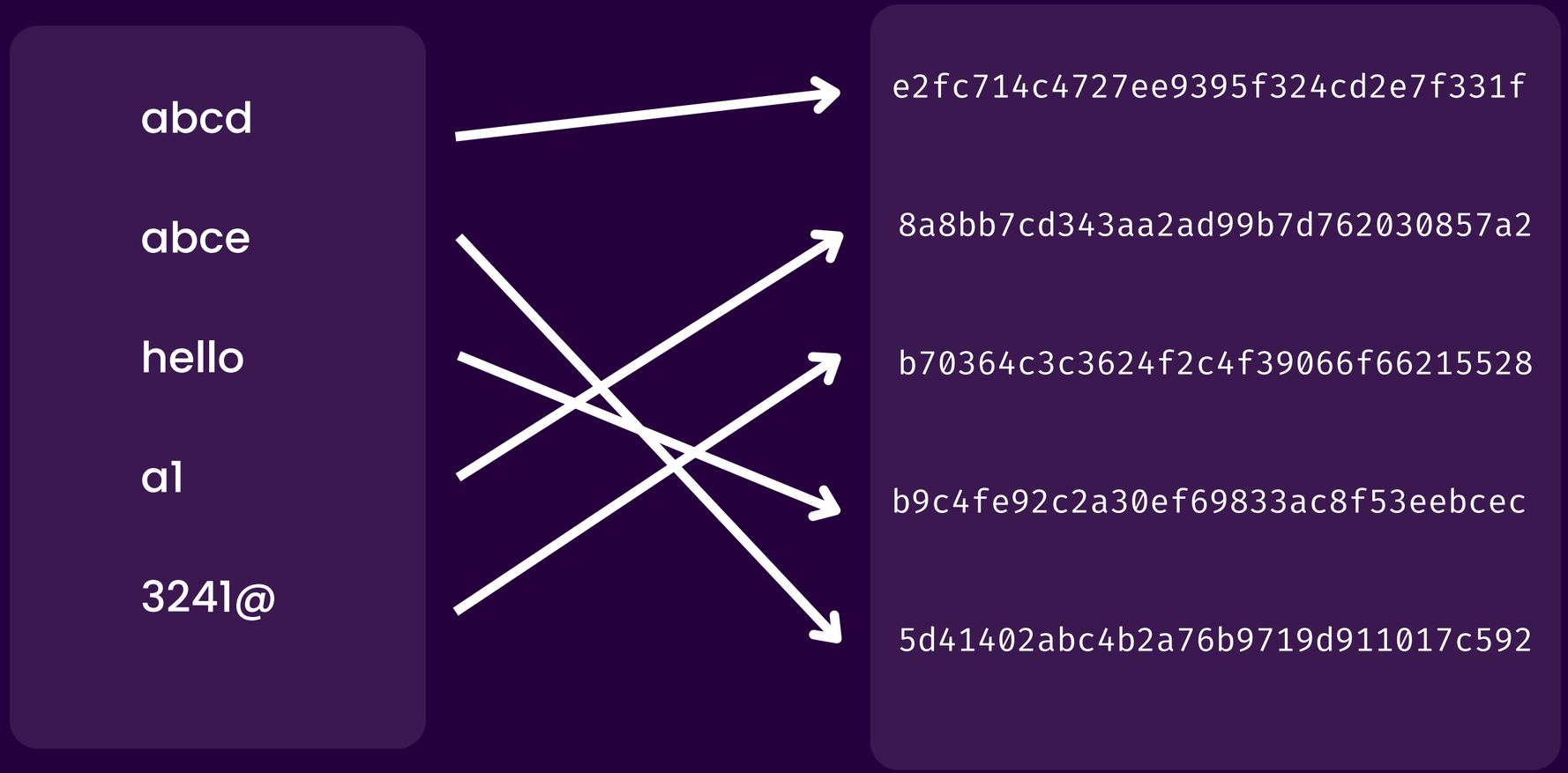
WLUG
COMMUNITY | KNOWLEDGE | SHARE

IRREVERSIBILITY

Hash Function

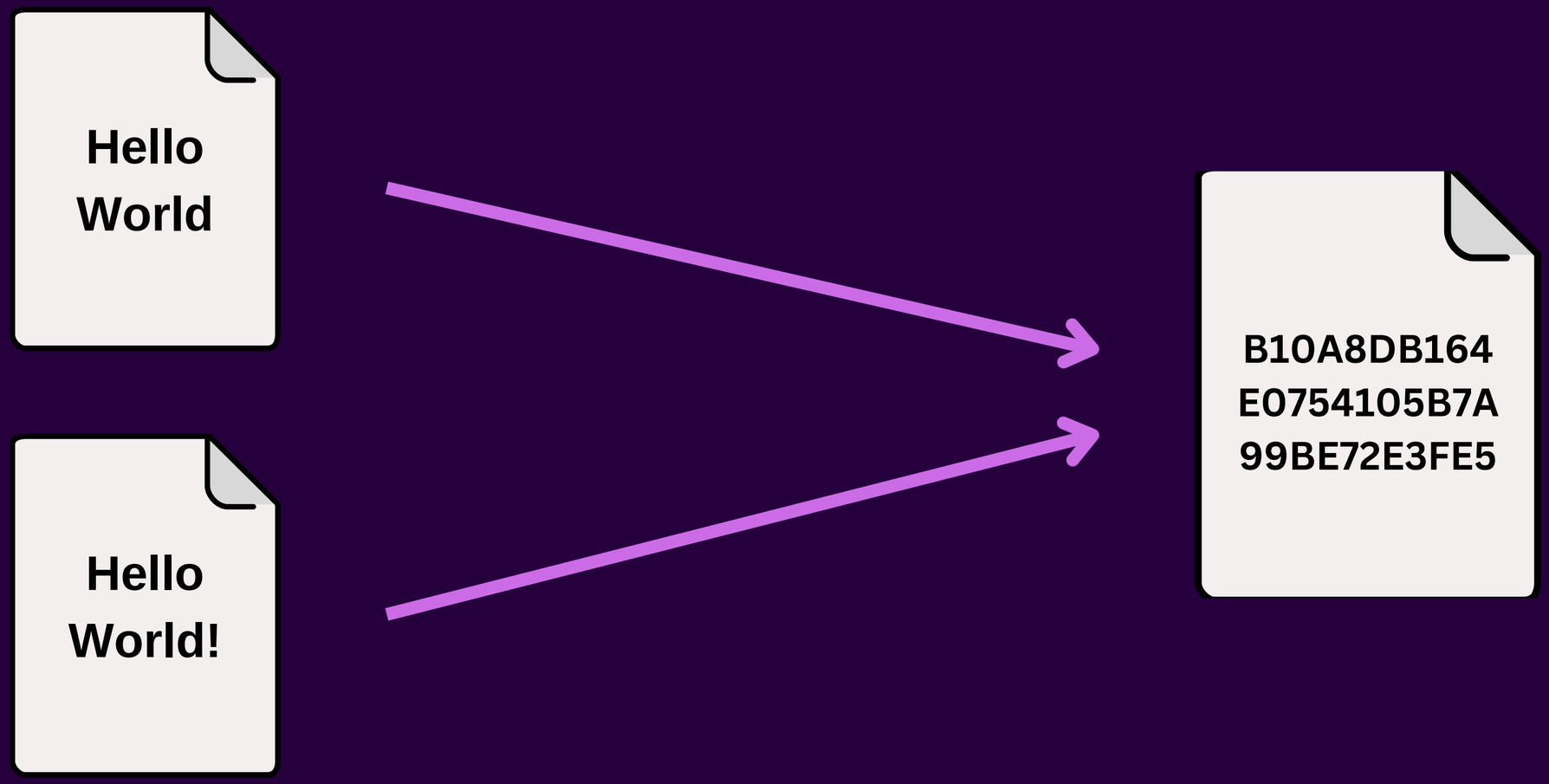
WLUG
COMMUNITY | KNOWLEDGE | SHARE

PSEUDORANDOMNESS



WLUG
COMMUNITY | KNOWLEDGE | SHARE

COLLISION RESISTANCE



WLUG
COMMUNITY | KNOWLEDGE | SHARE

FILE INTEGRITY

WLUG
COMMUNITY | KNOWLEDGE | SHARE

VERSION CONTROL

```
bhakti@bhakti in repo: Cryptography on  master took 30s
λ git log
commit c23727a147c87983ba90c35d7f3c007e84c1d86b (HEAD → master, origin/master, origin/HEAD)
Author: rakeshsukla53 <rakesh.sukla53@gmail.com>
Date:   Sun Dec 13 06:47:34 2015 -0500

    Quantum Crytography

commit 3dd0744bfe84b8baad020ef28b4206d9427e71cd
Author: rakeshsukla53 <rakesh.sukla53@gmail.com>
Date:   Sat Dec 12 03:56:28 2015 -0500

    Quantum Crytography

commit d35c0c84b3a839ff3de3e5ae5c8944700e377a39
Author: rakeshsukla53 <rakesh.sukla53@gmail.com>
Date:   Mon Nov 30 21:46:03 2015 -0500

    Quantum Crytography

commit 47aa095c1e7b18f2f1c49e5ab0c8e89031a892a3
Author: rakeshsukla53 <rakesh.sukla53@gmail.com>
Date:   Mon Nov 30 21:41:17 2015 -0500

    Discrete Logarthimic Problem

commit 658fd0c5f0b2eb36a3e25d93b24bae09ab1138d5
Author: rakeshsukla53 <rakesh.sukla53@gmail.com>
Date:   Mon Nov 30 18:21:07 2015 -0500

    Discrete Logarthimic Problem

commit c265edcc164cf9c9225f042d068eaf7f74764c1e
Author: rakeshsukla53 <rakesh.sukla53@gmail.com>
Date:   Mon Nov 30 18:15:48 2015 -0500

    Discrete Logarthimic Problem
```

```
bhakti@bhakti in repo: Cryptography on master as took 0s
λ docker pull alpine
Using default tag: latest
latest: Pulling from library/alpine
38a8310d387e: Pull complete
Digest: sha256:21dc6063fd678b478f57c0e13f47560d0ea4eeba26dfc947b2a4f81f686b9f45
Status: Downloaded newer image for alpine:latest
docker.io/library/alpine:latest

bhakti@bhakti in repo: Cryptography on master as took 21s
λ docker images --digests
REPOSITORY   TAG       DIGEST                                                                    IMAGE ID       CREATED      SIZE
alpine       latest    sha256:21dc6063fd678b478f57c0e13f47560d0ea4eeba26dfc947b2a4f81f686b9f45   4048db5d3672   7 days ago   7.83MB
```

WLUG
COMMUNITY | KNOWLEDGE | SHARE

PASSWORDS

Checksum

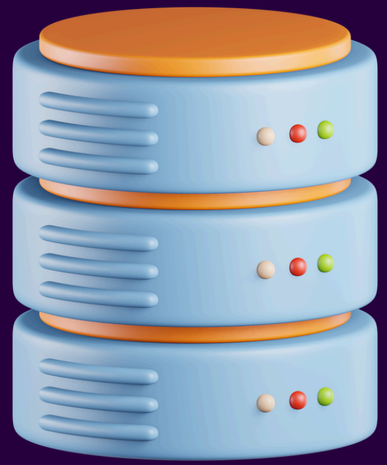
MD5

SHA-256

Doctor's prescription note

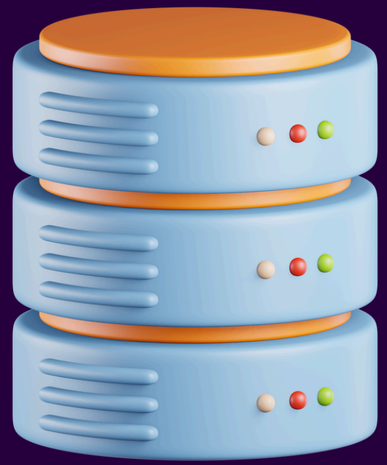
WLUG
COMMUNITY | KNOWLEDGE | SHARE

PASSWORDS



WLUG
COMMUNITY | KNOWLEDGE | SHARE

PASSWORDS



WLUG
COMMUNITY | KNOWLEDGE | SHARE

PASSWORDS

```
_id: ObjectId('675b1be342fa85c015ff191d')
username : "nova"
password : "pass@123"
__v : 0
```

Plain Text

WLUG
COMMUNITY | KNOWLEDGE | SHARE

PASSWORDS

```
_id: ObjectId('675b1c4265161d7e480de155')
username : "nova2"
password : "$2b$04$kpw9Rqrpm1qWhCprI403n.hnbE9l2WMscJgMDMVGsr7h4f1R3dWce"
__v : 0
```

Hashed Password

WLUG
COMMUNITY | KNOWLEDGE | SHARE

PASSWORDS WITH HASH

Username: nova

Password: pass@123

WLUG
COMMUNITY | KNOWLEDGE | SHARE

PASSWORDS WITH HASH

Username: nova

Password: pass@123

Database

hnbE912WMscJgMDM

WLUG
COMMUNITY | KNOWLEDGE | SHARE

PASSWORDS WITH HASH

Username: nova

Password: pass@123

Database

hnbE912WMscJgMDM

hnbE912WMscJgMDM

WLUG
COMMUNITY | KNOWLEDGE | SHARE

PASSWORDS WITH HASH

Username: nova

Password: pass@123

Database

hnbE912WMscJgMDM

hnbE912WMscJgMDM

hnbE912WMscJgMDM

WLUG
COMMUNITY | KNOWLEDGE | SHARE

PASSWORDS WITH HASH

Username: nova

Password: pass@123

Database

hnbE912WMscJgMDM

hnbE912WMscJgMDM

WLUG
COMMUNITY | KNOWLEDGE | SHARE

HASHING WITH SALTING

```
_id: ObjectId('675b1e70326528024d6497cd')
username : "nova3"
password : "$2b$10$M4Q8HjcymVBjrUq51e5qeu5ytD/FChKAnQpKTGHrFRqNSUC/TyGYK"
__v : 0
```

Hashed Password with Salt

WLUG
COMMUNITY | KNOWLEDGE | SHARE

HASHING WITH SALTING

Username: nova

Password: pass@123

Database

hfbgvr67

hnbE912WMscJgMDM

WLUG
COMMUNITY | KNOWLEDGE | SHARE

HASHING WITH SALTING

Database

Username: nova

Password: pass@123

hfbgvr67

hnbE912WMscJgMDM

pass@123

WLUG
COMMUNITY | KNOWLEDGE | SHARE

HASHING WITH SALTING

Username: nova

Password: pass@123

Database

hfbgvr67

hnbE912WMscJgMDM

pass@123 hfbgvr67

WLUG
COMMUNITY | KNOWLEDGE | SHARE

HASHING WITH SALTING

Database

Username: nova

Password: pass@123

hfbgvr67

hnbE912WMscJgMDM

hnbE912WMscJgMDM

WLUG
COMMUNITY | KNOWLEDGE | SHARE

HASHING WITH SALTING

Database

Username: nova

Password: pass@123

hfbgvr67

hnbE912WMscJgMDM

hnbE912WMscJgMDM

hnbE912WMscJgMDM

WLUG
COMMUNITY | KNOWLEDGE | SHARE

HASHING WITH SALTING

Username: nova

Password: pass@123

Database

hfbgvr67

hnbE912WMscJgMDM

hnbE912WMscJgMDM

WLUG
COMMUNITY | KNOWLEDGE | SHARE

THANK YOU

Community | Knowledge | Share

The Cipher Show

Ameya Unchgaonkar

Bhakti More

Aditya Aparadh