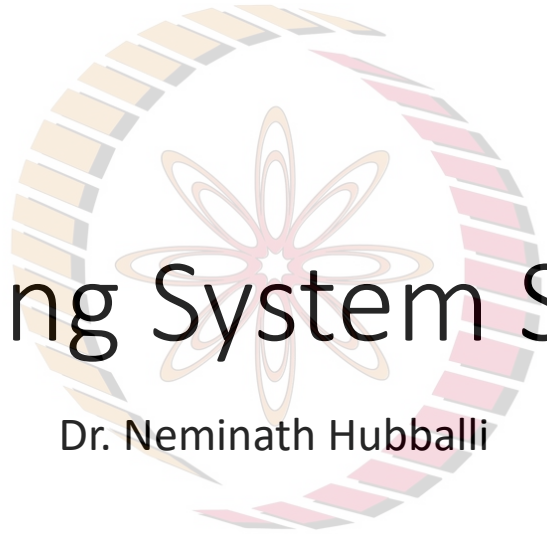


The NPTEL logo is a circular emblem. It features a central stylized flower or star shape with eight petals, rendered in a light pink and orange color. This central motif is surrounded by a circular border composed of alternating orange and pink segments, creating a segmented or gear-like appearance.

Operating System Security

Dr. Neminath Hubballi

NPTEL

Outline

- ☐ Memory Management
- ☐ Password and User Account Management



Memory Management

- ❑ Process granularity
 - ❑ Each process upon creation is allocated some memory called as address space
 - ❑ Operating system protects one process from other by not allowing access to others address space
- ❑ Global granularity
 - ❑ Kernel address space
 - ❑ User address space

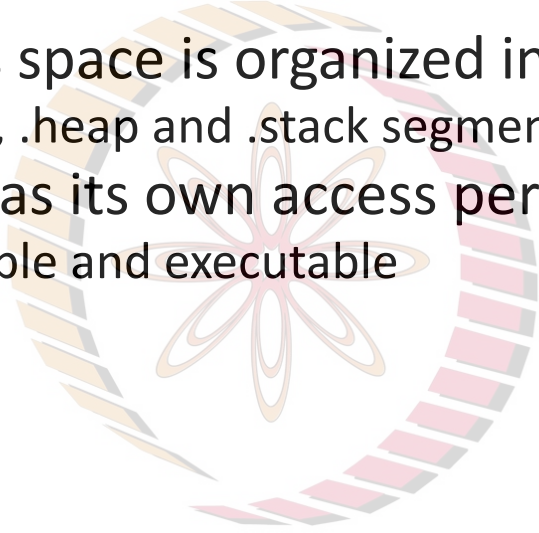
NPTTEL

Memory Management



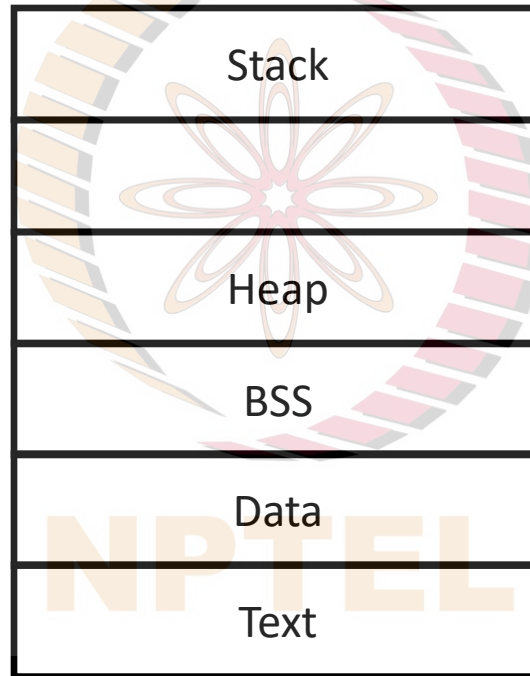
Memory Management

- ❑ Process address space is organized in segments
 - ❑ .text, .data, .bss, .heap and .stack segments
- ❑ Each segment has its own access permissions
 - ❑ Readable, writable and executable

The NPTEL logo is a circular emblem. It features a stylized lotus flower in the center, with eight petals. Surrounding the lotus is a ring composed of many small, rectangular segments, some of which are colored in shades of orange and pink. Below the emblem, the word "NPTEL" is written in a bold, sans-serif font, with the letters in a light orange color.

NPTEL

Memory Management



Examples

Heap

```
int main()
{
    ptr = (int *) malloc(10*sizeof(int));
}
```

.bss

```
int main()
{
    static int a;
}
```

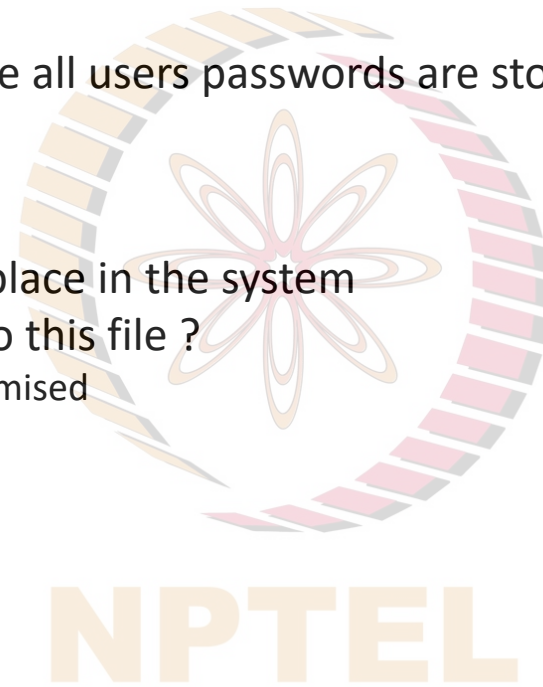
.data

```
int gb=10;
int main()
{
}
```



Password and User Account Management in Operating System

- ❑ Naive approach
 - ❑ Create a file password where all users passwords are stored
 - ❑ Neminath : pass156
 - ❑ Gourinath : test234
 - ❑ Somnath : temp123
 - ❑ Save the file password in a place in the system
 - ❑ What if a thief gets access to this file ?
 - ❑ All user accounts are compromised



Password and User Account Management in Operating System



Password and User Account Management in Operating System



Password and User Account Management in Operating System



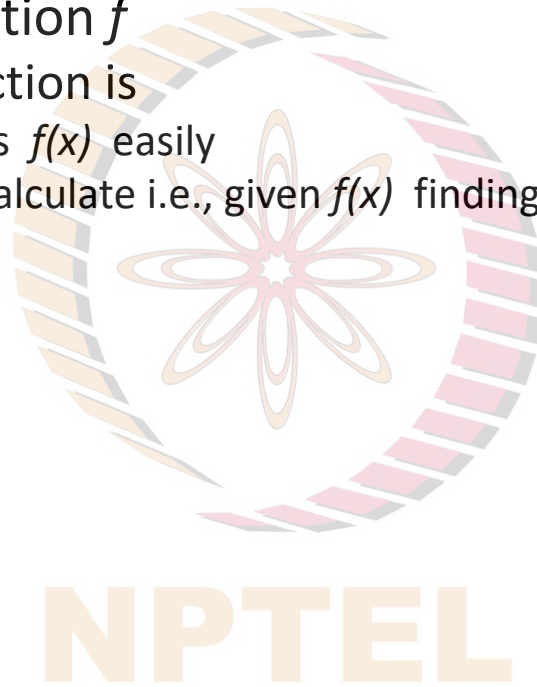
Password and User Account Management in Operating System

- ❑ One way hashing is a function f
- ❑ Characteristic of this function is
 - ❑ when supplied x computes $f(x)$ easily
 - ❑ But inverse is extremely complex i.e., given $f(x)$ it is difficult to calculate x .
 - ❑ Somanath : d34ef



Password and User Account Management in Operating System

- ❑ One way hashing is a function f
- ❑ Characteristic of this function is
 - ❑ when supplied x computes $f(x)$ easily
 - ❑ But inverse is difficult to calculate i.e., given $f(x)$ finding x .
 - ❑ Somanath : d34ef



Password and User Account Management in Operating System

- ❑ One way hashing is a function f
 - ❑ Characteristic of this function is
 - ❑ when supplied x computes $f(x)$ easily
 - ❑ But inverse is extremely complex i.e., given $f(x)$ it is difficult to calculate x .
 - ❑ Somanath : d34ef
- ❑ An example
 - ❑ Convert all the characters into their ASCII values and XOR them
 - ❑ Result is a small number derived out of XOR operation
 - ❑ Store the hash value in password file
 - ❑ Note we do not store the password anywhere
 - ❑ The idea is make it impossible to guess the password even if hash value is known
 - ❑ Now the password file looks like
 - ❑ Neminath : a12hf
 - ❑ Gourinath : b4a2e

Password and User Account Management in Operating System



Password and User Account Management in Operating System



Password and User Account Management in Operating System

☐ Salting

- ☐ Do not hash passwords as it is, add something to it and then hash
- ☐ Unix system used an additional 12 bit number to hash password
- ☐ How to chose value of salt
 - ☐ Deterministic across the users: not a good idea !
 - ☐ Unique for each user : sounds good but how to get a unique one
 - ☐ Take the current timestamp of system and divide with a predetermined number to get a 12 bit remainder and use it as a salt.
 - ☐ Meta data as salt : use the birthday or PAN number of user as salt

Password and User Account Management in Operating System



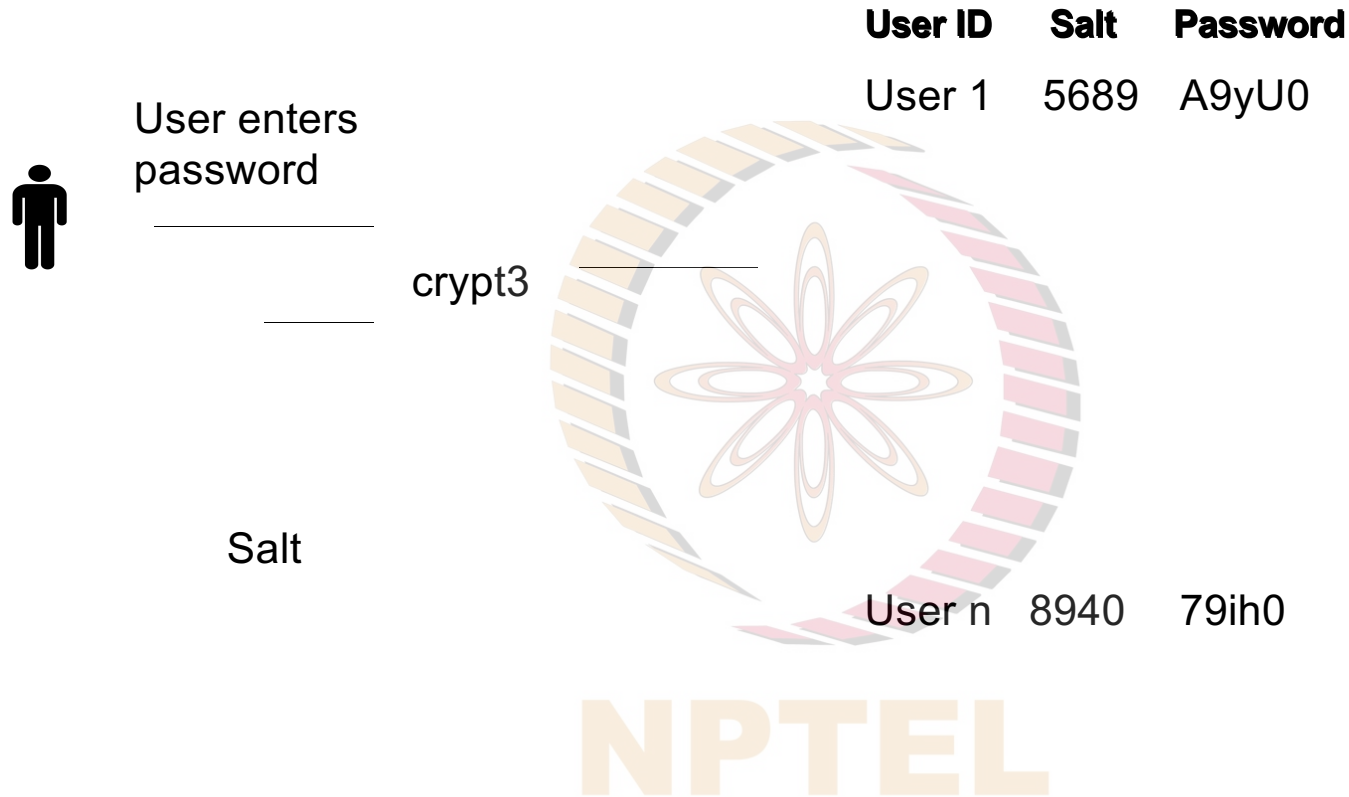
Unix Password Management

- ❑ A file in the directory `/etc/passwd` stores the Unix users password
- ❑ Unix password is hashed and salted
- ❑ Salting and hashing effectively increase the amount of work done to break into the target system
- ❑ Algorithm
 - ❑ Take the first 8 ASCII characters of the user password and encrypt a 64 bit constant character consisting of all 0's
 - ❑ If the user password is less than 8 characters suitably pad it to make it 56 bits
 - ❑ Encrypt the 64 bit length 0's 25 times with DES (**using crypt() function**) using user password as key
 - ❑ Resultant encrypted version is stored in the file

Unix Password Management

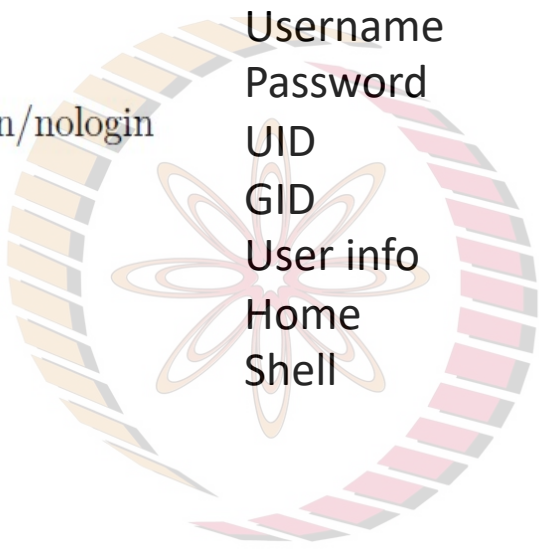


Password Management in Unix/Linux



Where is the Hashed Password Stored ?

```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
```



A diagram showing a circular structure with a flower-like center. The center is divided into segments, each labeled with a field from a password entry. The labels are: Username, Password, UID, GID, User info, Home, and Shell. The circular structure is composed of yellow and pink segments.

Username
Password
UID
GID
User info
Home
Shell

```
$ sudo cat /etc/shadow
root!:16903:0:99999:7:::
daemon*:16652:0:99999:7:::
bin*:16652:0:99999:7:::
sys*:16652:0:99999:7:::
user1:$6$j6I6L8Mi$.zx.45fgRT7776598/:16903:0:99999:7:::
```

NPTTEL

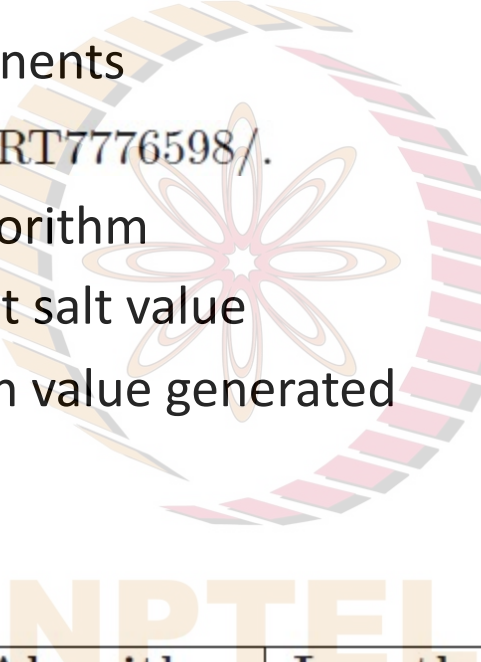
Username
Encrypted Password
Elapsed time
Validity
Due date
Warning date
Expiry date
Disabled time
Reserved

Where is Hashed Password Stored ?

- ❑ Password has 3 components

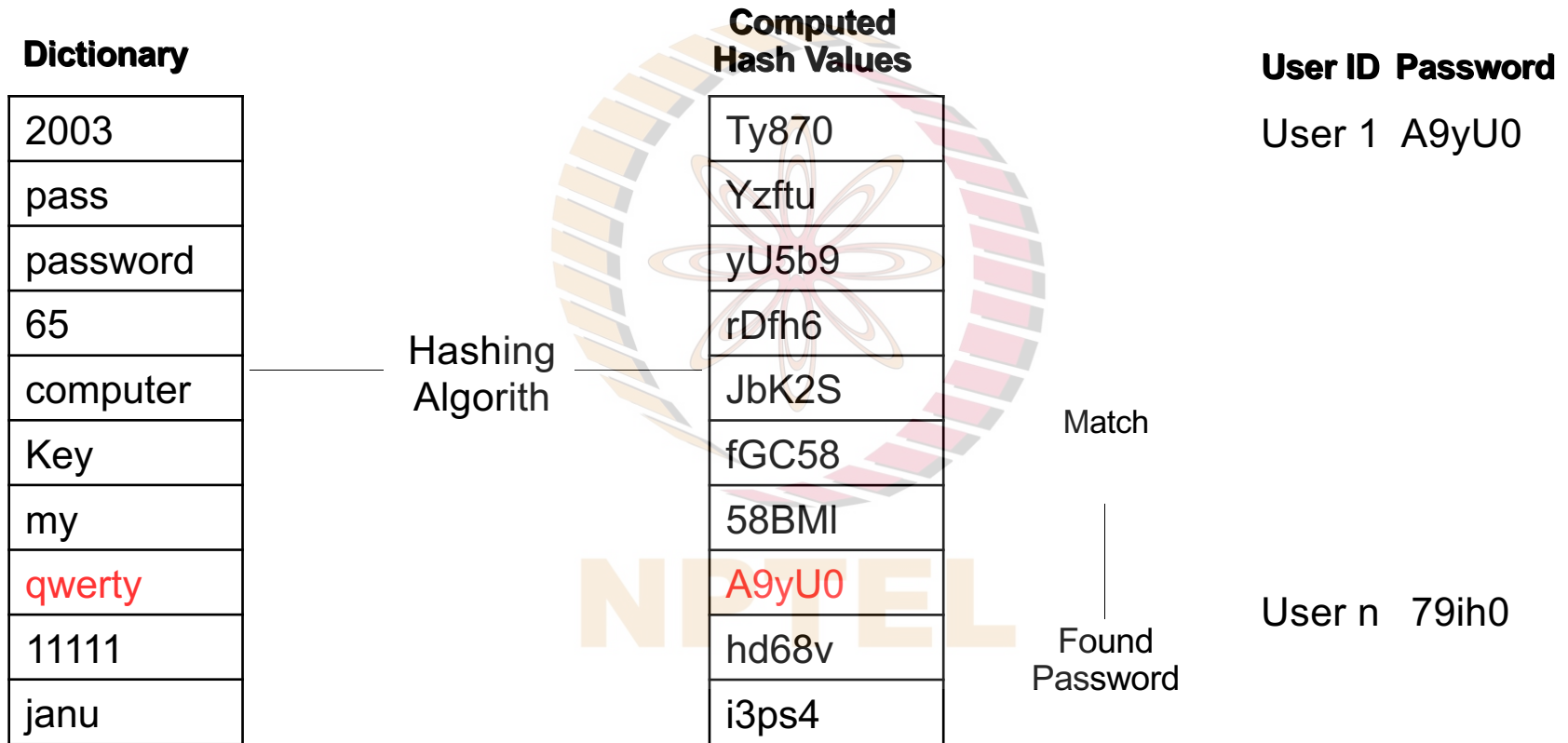
\$6\$j6I6L8Mi\$.zx.45fgRT7776598/.

- ❑ First part – hashing algorithm
- ❑ Second part – plain text salt value
- ❑ Third part – actual hash value generated

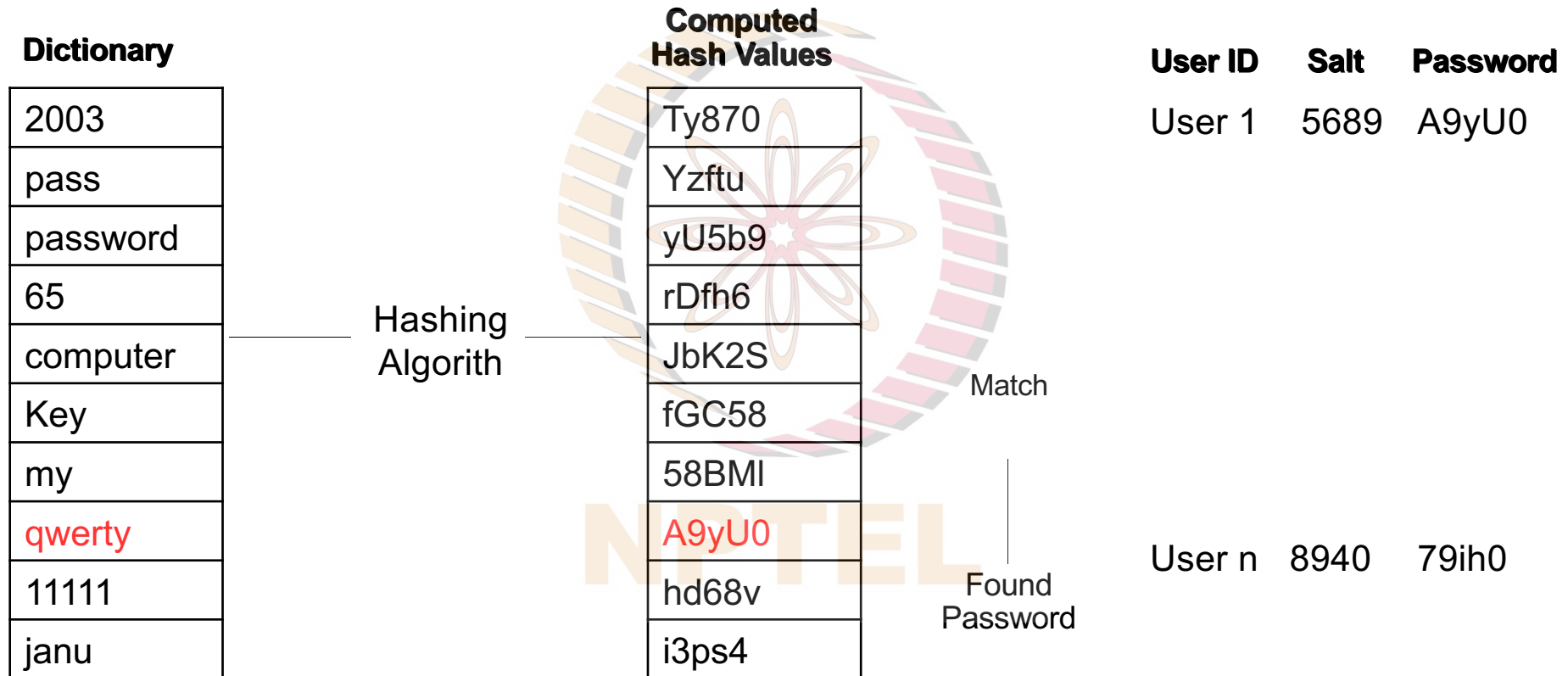


ID	Algorithm	Length
1	MD5	22 Characters
2a	Blowfish	12 Characters
5	SHA-256	43 Characters
6	SHA-512	86 Characters

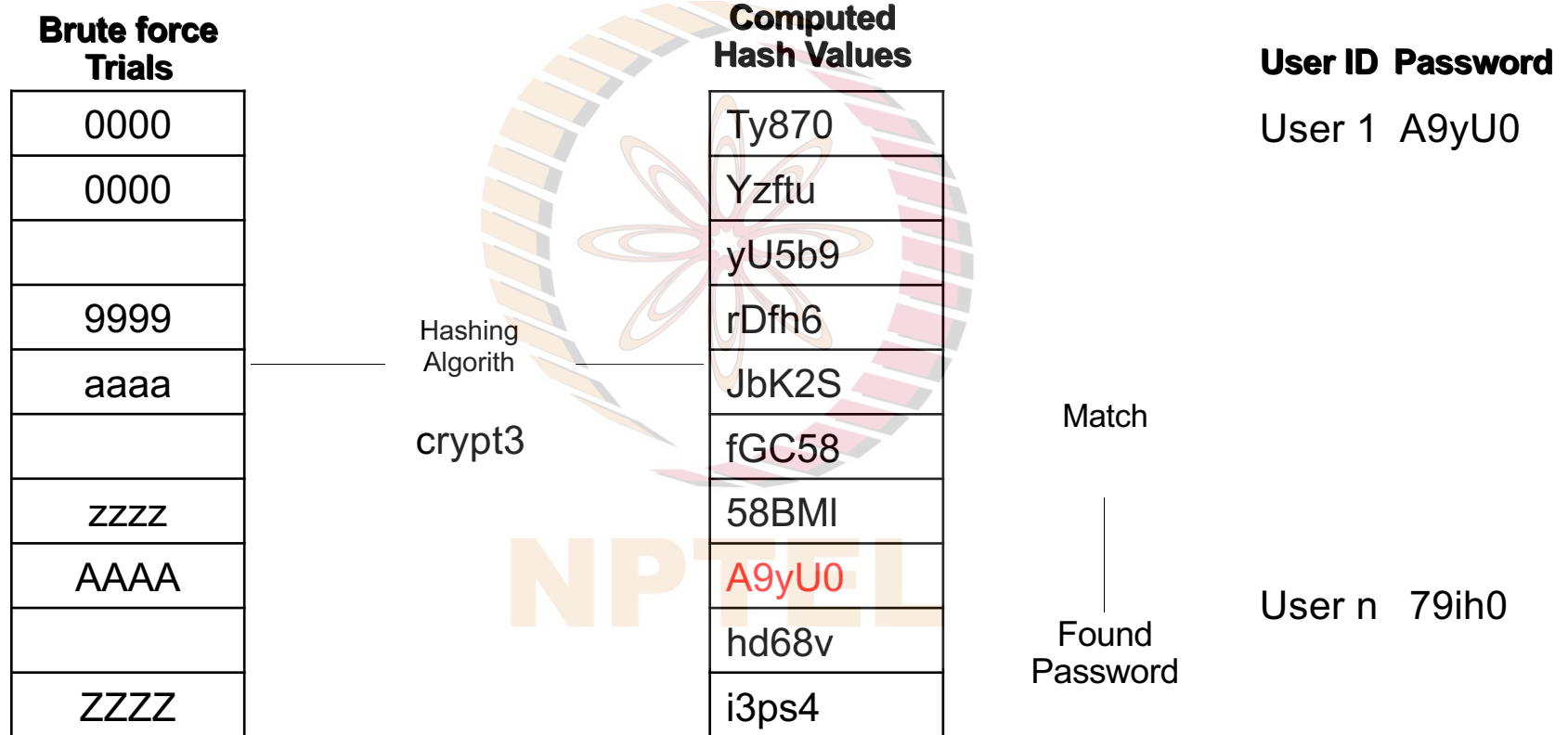
Attacks on Password based Authentication



Attacks on Password based Authentication



Attacks on Password based Authentication



Attacks on Password based Authentication

