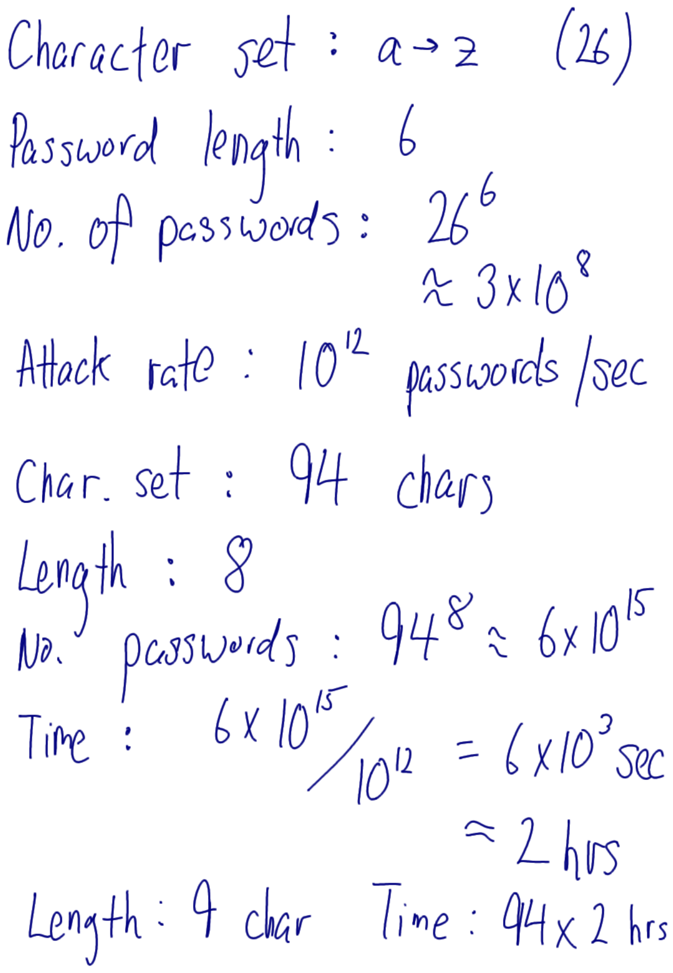
CSS322 – Passwords Notes



Character set : a → z (26)

Password length : 6

No. of passwords : 26^6

$\approx 3 \times 10^8$

Attack rate : 10^{12} passwords/sec

Char. set : 94 chars

Length : 8

No. passwords : $94^8 \approx 6 \times 10^{15}$

Time : $6 \times 10^{15} / 10^{12} = 6 \times 10^3$ sec

≈ 2 hrs

Length : 9 char Time : 94 x 2 hrs

Figure 1: Password brute force examples; Lecture 25

8 passwords	000 001 010 ⋮ 111 3 bits
10 passwords	4 bits
n passwords	$\log_2(n)$ bits
3×10^8 passwords	28.16 bits (29)
1 character, a → z (26)	$\log_2(26)$ $= 4.70$
1 char, 0 → 9 (10)	3.32
10 char, a → z	$4.70 \times 10 = 47.0$ bits
14 char, 0 → 9	47 bits

Figure 2: Password entropy examples; Lecture 25

# of passwords: 94^{10}

Entropy: $\log_2(94^{10})$

≈ 65.9

Figure 3: Password Entropy Example; Lecture 26

username	password
john	mysecret
sandy	1d9a%23f
daniel	mysecret
...	...
steve	h31p_m3?

Figure 4: Password Storage - Cleartext password; Lecture 26

username	~~password~~	$E(K_S, password)$
john	~~mysecret~~	aXj4 ......
sandy	~~1d9a%23f~~	......
daniel	~~mysecret~~	2Z34j....
...	~~...~~	
steve	~~h31p_m3?~~	......

$C = E(K = mysecret, P = mysecret)$

Submit john, mysecret:

$P = D(mysecret, C)$

Figure 5: Password Storage - Encrypted; Lecture 26

username	H(password)
john	06c219e5bc8378f3a8a3f83b4b7e4649
sandy	5fc2bb44573c7736badc8382b43fbeae
daniel	06c219e5bc8378f3a8a3f83b4b7e4649
...	...
steve	75127c78fd791c3f92a086c59c71ece0

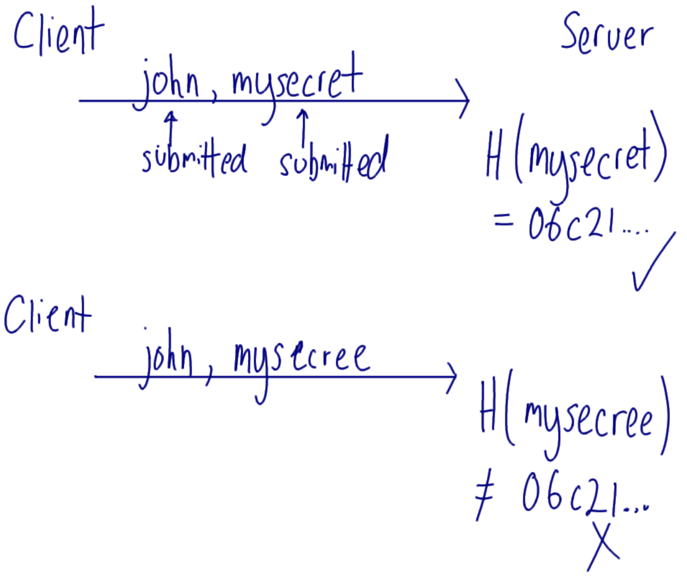
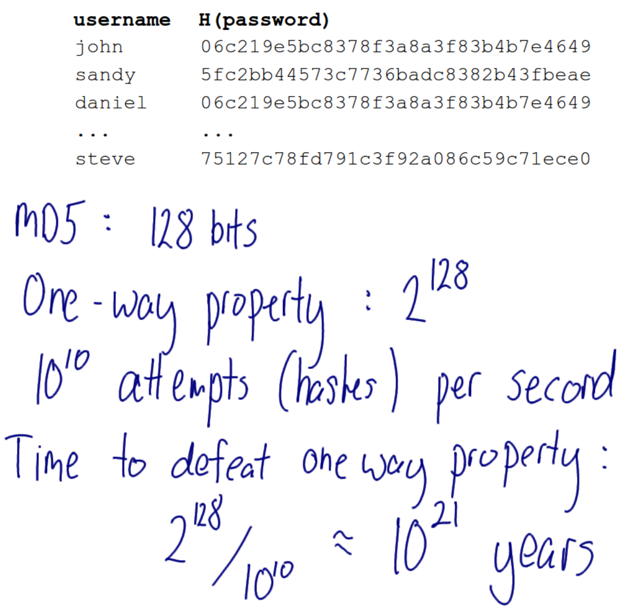


Figure 6: Password Storage - Hash of password; Lecture 26



```
username   H(password)
john       06c219e5bc8378f3a8a3f83b4b7e4649
sandy      5fc2bb44573c7736badc8382b43fbeae
daniel     06c219e5bc8378f3a8a3f83b4b7e4649
...        ...
steve      75127c78fd791c3f92a086c59c71ece0
```

MD5 : 128 bits

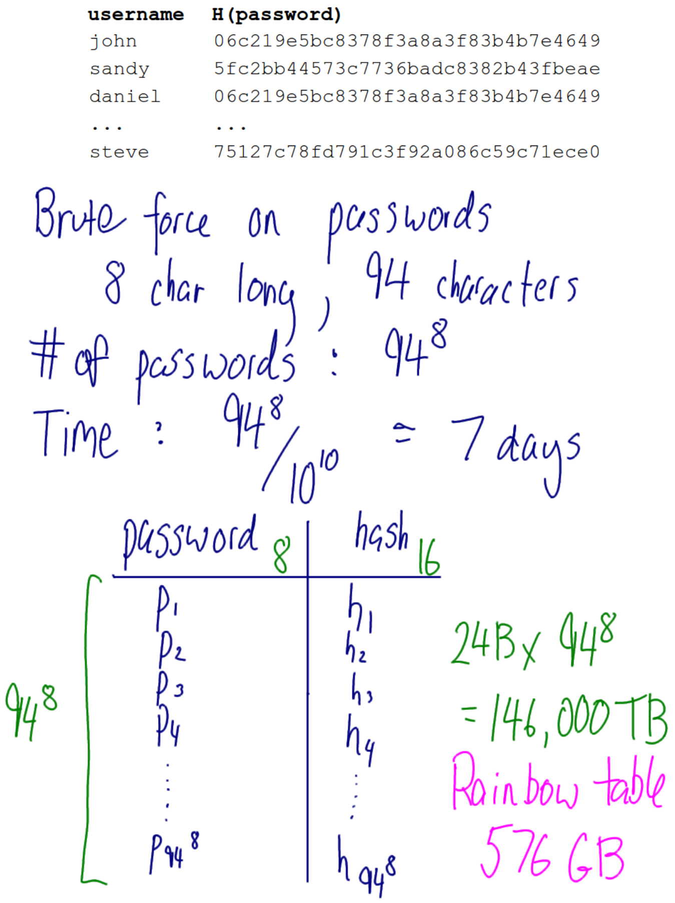
One-way property : 2^{128}

10^{10} attempts (hashes) per second

Time to defeat one way property :

$2^{128}/10^{10} \approx 10^{21}$ years

Figure 7: Password Storage - Brute Force on Hash; Lecture 26



```
username   H(password)
john       06c219e5bc8378f3a8a3f83b4b7e4649
sandy      5fc2bb44573c7736badc8382b43fbeae
daniel     06c219e5bc8378f3a8a3f83b4b7e4649
...        ...
steve      75127c78fd791c3f92a086c59c71ece0
```

Brute force on passwords

8 char long, 94 characters

# of passwords : 94^8

Time : $94^8/10^{10} \simeq 7$ days

password 8	hash 16
p_1	h_1
p_2	h_2
p_3	h_3
p_4	h_4
$\vdots$	$\vdots$
p_{94^8}	h_{94^8}

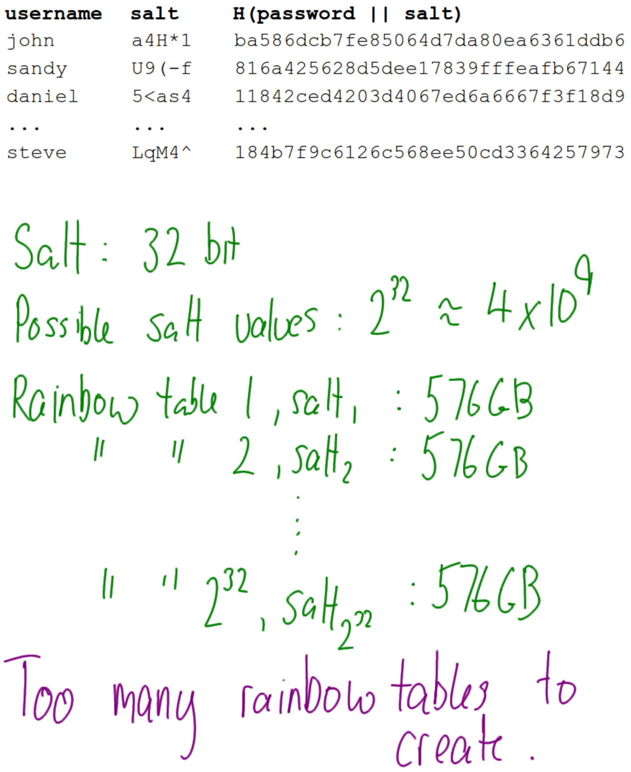
24B x 94^8

= 146,000 TB

Rainbow table

576 GB

Figure 8: Password Storage - Using Rainbow Table; Lecture 26



username	salt	H(password || salt)
john	a4H*1	ba586dcb7fe85064d7da80ea6361ddb6
sandy	U9(-f	816a425628d5dee17839fffeafb67144
daniel	5<as4	11842ced4203d4067ed6a6667f3f18d9
...	...	...
steve	LqM4^	184b7f9c6126c568ee50cd3364257973

Salt: 32 bit

Possible salt values: $2^{32} \approx 4 \times 10^9$

Rainbow table 1, salt$_1$: 576GB

" " 2, salt$_2$: 576GB

⋮

" " 2^{32}, salt$_{2^{32}}$: 576GB

Too many rainbow tables to create.

Figure 9: Password Storage - Salted Hash; Lecture 26