

# AIX Password Cracking with John

AIX is the IBM UNIX and information is available at <http://www.ibm.com/aix>

The purpose of this page is:

- to show information about DES cracking and why password policies are important

The results might be used to estimate cracking workloads for other UNIX platforms that use DES for encrypting passwords, but was performed using passwd entries from AIX 5.3.

## AIX passwords

AIX by default uses passwords with a max length of 8 characters and uses the old crypt algorithm based on DES.

This make password files from AIX relatively easy to crack using a password cracker like John the Ripper.

## Easy digits

Digits are the numbers from 0 to 9: 0123456789

How long does it take to try out all combinations from 0 to 99999999?

The number of possible combinations are:  $8^8 = 16777216$  and since my cracker Sylvester does about 700.000 c/s with John it doesn't take long.

I made a couple of test password files using AIX having only a single password each. The one named passwd.abcdefgh having only a single password hash of the password abcdefgh - which is NOT only digits. Running John with this as input and selecting incremental mode with digits only it will not crack this password, but will try all combinations of digits.

The results from a real run on Sylvester:

```
hlk@sylvester:hlk$ cd pwd
hlk@sylvester:pwd$ ls
Makefile          john.conf         passwd.12345678  passwd.abcdefgh
wordlists
hlk@sylvester:pwd$ cat passwd.abcdefgh
user01:JizPRGLdRtePs:0:0:Unix Admin:/root:/usr/bin/ksh
hlk@sylvester:pwd$ cat passwd.12345678
user02:cfBzVeHe4j/OQ:0:0:Unix Admin:/root:/usr/bin/ksh
hlk@sylvester:pwd$ cat passwd.abcdefgh passwd.12345678 > passwd
hlk@sylvester:pwd$ time john -incremental:digits passwd
Created directory: /home/hlk/.john
Loaded 2 password hashes with 2 different salts (Traditional DES [64/64
BS])
12345678          (user02)
```

## Default Publication

```
guesses: 1   time: 0:00:02:41   c/s: 687559   trying: 83536787 - 83536784
          2m41.61s real      2m40.29s user      0m0.11s system
h1k@sylvester:pwd$
```

Note that the password 12345678 was found almost immediately due to the way John cracks passwords.

## Better alpha a-z lower case - but still easy

So digits are toast, but what about the letters a-z lower case.

How long would it take to try out all combinations from a to zzzzzzzz?

The number of combinations are  $26^8 = 208827064576$  and using again sylvester and 700.000 c/s it is

$208827064576 / 700000$  seconds = 298324 seconds = ~ 82 hours roughly 3-4 days, give or take.

I have started Sylvester with the same passwd file, the one with passwords abcdefgh and 12345678 and it found the first one within minutes, but the other one is NOT within a-z - so John will have to try all combinations

```
$ cd pwd
$ time john -incremental:alpha passwd
Created directory: /home/h1k/.john
Loaded 2 password hashes with 2 different salts (Traditional DES [64/64
BS])
abcdefg      (user01) // found within minutes
...
come back later and see the results!
```

## Notes

Remember to remove .john between runs, if you do multiple runs of the same password files - as it saves the passwords it has found and can restore sessions that you interrupt.