

# Projekt om lösenordsknäckande

December 2003 – Martin Fahlgren  
Av Per Hillerström och Erik Bane

---

## John The Ripper

Program som John The Ripper knäcker lösenord och baseras på en enkel idé. Det finns ordlistor att tanka hem. Med hjälp av dessa ordlistor försöker programmet med alla ord i ordlistan och sedan med variationer av dessa ord. De krypterar var och ett och kollar det mot ditt krypterade lösenord. Om det stämmer så är de inne.

Ett litet urklipp ur en sådan ordlista som finns för flera olika språk, detta är en svensk:  
Adrenalinadressadressatadressateradresseradvokatadvokatyraffischaffischeraff{  
JennyJernbergJoachimJohanJohnJohnnyJokernJonasson

John The Ripper kan klara av att cracka lösenord från:

- Standard DES
- BSDI DES
- FreeBSD MD5
- OpenBDS Blowfish
- Kerberos AFS DES
- NT LM DES

John The Ripper samt diverse andra program som knäcker lösenord använder mycket av din CPU-tid. För att en hacker skall få en chans att kunna köra John The Ripper på din dator måste det finnas en säkerhetsläcka som man kan komma in i dator på. Ofta är ju dessa vanligare än vad man tror.

Programmet finns för UNIX, DOS samt även för Windows 32-bitars, finns att hämta på dessa nedan angivna adresser.

- <http://www.openwall.com/john/a/john-16w.zip> (Windows 32-bit)
- <http://www.openwall.com/john/a/john-16d.zip> (DOS)
- <http://www.openwall.com/john/a/john-1.6.tar.gz> (UNIX)

Senaste versionen som finns tillgänglig är 1.6.36 (19 september 2003)

```
C:\Program\ripper\john-16w\run>john
John the Ripper Version 1.6 Copyright (c) 1996-98 by Solar Designer
Usage: john [OPTIONS] [PASSWORD-FILES]
-single "single crack" mode
-wordfile:FILE -stdin wordlist mode, read words from FILE or stdin
-rules enable rules for wordlist mode
-incremental[:MODE] incremental mode [using section MODE]
-external:MODE external mode or word filter
-stdout[:LENGTH] no cracking, just write words to stdout
-restore[:FILE] restore an interrupted session [from FILE]
-session:FILE set session file name to FILE
-status[:FILE] print status of a session [from FILE]
-makechars:FILE make a charset, FILE will be overwritten
-show show cracked passwords
-test perform a benchmark
-users:[-ILOGIN!UID[,...]] load this (these) user(s) only
-groups:[-IGID[,...]] load users of this (these) group(s) only
-shells:[-ISHELL[,...]] load users with this (these) shell(s) only
-salts:[-ICOUNT] load salts with at least COUNT passwords only
-format:NAME force ciphertext format NAME (DES/BSDI/MD5/BF/AFS/LM)
-savemem:LEVEL enable memory saving, at LEVEL 1..3
```

John The Ripper in action

```
D:\WINNT\system32\cmd.exe - john test.txt
D:\john\john-16w\run>john test.txt
Loaded 2 passwords with 2 different salts (Standard DES [48/64 4K])
guesses: 0 time: 0:00:00:04 (3) c/s: 65011 trying: mondan1 - spokale
guesses: 0 time: 0:00:00:05 (3) c/s: 65090 trying: shopeR - babor1
guesses: 0 time: 0:00:00:08 (3) c/s: 73417 trying: pum90 - pruga
guesses: 0 time: 0:00:00:09 (3) c/s: 79809 trying: parielas - portimon
guesses: 0 time: 0:00:00:11 (3) c/s: 77202 trying: pkat - phde
guesses: 0 time: 0:00:00:21 (3) c/s: 96558 trying: 15415 - tbc11
guesses: 0 time: 0:00:00:29 (3) c/s: 101528 trying: cathares - shothiri
guesses: 0 time: 0:00:00:38 (3) c/s: 105049 trying: mutacol - beove90
guesses: 0 time: 0:00:00:47 (3) c/s: 107222 trying: bb3em - ribup
```

Detta är resultatet efter att John The Ripper nästan gjort sitt jobb

```
D:\john\john-16w\run>john -show test.txt
satu:4567
io:daniel
jukka:hora
annica:annica
janson:hiatch

5 passwords cracked, 2 left
D:\john\john-16w\run>
```

## C r a c k

Likaså detta program är ett lösenordsknäckar program och är skrivet av Alec Muffett. Programmet Crack fungerar ungefär som John the ripper men finns bara till UNIX el Linux. Crack är ett litet, snabbt, flexibelt och konfigurerbart program för att knäcka DES krypterade lösenord.