

**John the Ripper** is a [free](https://en.wikipedia.org/wiki/Free_software) [password cracking](https://en.wikipedia.org/wiki/Password_cracking) software tool.Originally developed for the [Unix operating system](https://en.wikipedia.org/wiki/Unix_operating_system), it can run on fifteen different platforms (eleven of which are architecture-specific versions of Unix, [DOS](https://en.wikipedia.org/wiki/DOS), [Win32](https://en.wikipedia.org/wiki/Microsoft_Windows), [BeOS](https://en.wikipedia.org/wiki/BeOS), and [OpenVMS](https://en.wikipedia.org/wiki/OpenVMS)). It is among the most frequently used password testing and breaking programs as it combines a number of password crackers into one package, [autodetects](https://en.wikipedia.org/w/index.php?title=Autodetection&action=edit&redlink=1) password [hash](https://en.wikipedia.org/wiki/Hash_function) types, and includes a customizable cracker. It can be run against various [encrypted](https://en.wikipedia.org/wiki/Encryption) password formats including several [crypt](https://en.wikipedia.org/wiki/Crypt_(Unix)) password hash types most commonly found on various Unix versions (based on [DES](https://en.wikipedia.org/wiki/Data_Encryption_Standard), [MD5](https://en.wikipedia.org/wiki/MD5), or [Blowfish](https://en.wikipedia.org/wiki/Blowfish_(cipher))), [Kerberos](https://en.wikipedia.org/wiki/Kerberos_(protocol)) [AFS](https://en.wikipedia.org/wiki/Andrew_File_System), and Windows NT/2000/XP/2003 [LM hash](https://en.wikipedia.org/wiki/LM_hash). Additional modules have extended its ability to include [MD4](https://en.wikipedia.org/wiki/MD4)-based password hashes and passwords stored in [LDAP](https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol), [MySQL](https://en.wikipedia.org/wiki/MySQL), and others.One of the modes John can use is the [dictionary attack](https://en.wikipedia.org/wiki/Dictionary_attack). It takes text string samples (usually from a file, called a wordlist, containing words found in a [dictionary](https://en.wikipedia.org/wiki/Dictionary) or real passwords cracked before), encrypting it in the same format as the password being examined (including both the encryption algorithm and key), and comparing the output to the encrypted string. It can also perform a variety of alterations to the dictionary words and try these. Many of these alterations are also used in John's single attack mode, which modifies an associated plaintext (such as a username with an encrypted password) and checks the variations against the hashes.

John also offers a [brute force](https://en.wikipedia.org/wiki/Brute_force_attack) mode. In this type of attack, the program goes through all the possible [plaintexts](https://en.wikipedia.org/wiki/Plaintext), hashing each one and then comparing it to the input [hash](https://en.wikipedia.org/wiki/Cryptographic_hash_function). John uses character frequency tables to try plaintexts containing more frequently used characters first. This method is useful for cracking passwords that do not appear in dictionary wordlists, but it takes a long time to run.

To know more:-

Cheat sheet:- <https://countuponsecurity.files.wordpress.com/2016/09/jtr-cheat-sheet.pdf>

Course:- <https://www.udemy.com/course/password-cracking-with-john-the-ripper/>

How to use:- <https://www.hackingarticles.in/beginner-guide-john-the-ripper-part-1/>

Video:- <https://youtu.be/XjVYl1Ts6XI?feature=shared> (©HackerSploit)