# *Once seen as bulletproof, 11 million+ Ashley Madison passwords*

# *already cracked*

In 2015, sketchy dating site Ashley Madison suffered an enormous breach of data when hackers dumped a lot of personal data gleaned from Ashley Madison databases including names, home addresses, search histories and credit card numbers of users. Among this were hashes of passwords associated with user accounts.

For quite a while it was believed that the passwords were secure. The passwords were hashed using a cryptographically secure hash function known as bcrypt, so that cracking the passwords would take centuries. However, a group known as CynoSure Prime has recently figured out how to get the passwords after discovering a separate hash that stored the passwords using the MD5 hashing function, which is considerably less secure than bcrypt.

The first step in recovering the account passwords was to crack the passwords stored as MD5 hashes. Since MD5 is extraordinarily fast, it can be broken with brute force. Ashley Madison converted all of the passwords to lowercase before storing them with MD5, so in order to get back the actual password in full, the attackers had to run the bcrypt algorithm on permutations of the password, changing letters to uppercase, until they found a match. Since they only had to run this on permutations of a password they almost already knew, this operation is much faster than trying every combination using bcrypt. So, if you got back “password” after brute forcing MD5, since there are 8 letters in password there are 28 ways of capitalizing different letters (ie “Password”, “pAssword”, “paSsword” etc), leading to a maximum of 256 passwords that need to be run through bcrypt.