# Crack me, I'm famous!: Cracking weak passphrases using freely available sources
# Appendix

Hugo Labrande
INRIA Nancy, Equipe CARAMEL University of Calgary, ISPIA

June 1, 2015

## 1 Other databases

One of the natural questions is whether the techniques described in the article also work for other dictionaries. The Korelogic database, although big, is considered a rather mediocre source of passwords; it is not clear where the passwords come from, how they have been harvested, and if there is some sort of bias, for instance. The original article cracked more than 4 million passwords out of 122 million; can this kind of result be replicated?

We report here trying the method on two more databases of MD5: the eHarmony and the Gamigo database, found on `http://www.adeptus-mechanicus.com/codex/hashpass/hashpass.php`. Both of those databases are cracked at more than 97%, with only tens of thousands left; running our dictionaries on them showed that the overwhelming majority of the passwords that we can find have already been found. This could mean that our methods are already known, but there is no way to confirm this since the methods (and dictionaries) used to crack those databases are not public; this is more likely to simply mean that some undisclosed method allows guessing most passwords, including famous passphrases. This could for example be accomplished by the methods of Dustin & Young, considering all the sentences in Wikipedia, crawling other online sources, etc. This does not change the fact that our method can be used by any attacker, even those with low skills, to build focused dictionaries in a short time.

Our results for those two databases are as follows: we cracked 100,473 passwords from the eHarmony database (out of 1,516,834, a 6.6% crack rate), and 384,951 from the Gamigo database (out of 7,004,341, a 5.5% crack rate), which is actually better percentage-wise than what we achieved with the Korelogic database. Of those, some do not appear to have been cracked before: we found 5 of them in the eHarmony database and 31 of them in the Gamigo database that were not part of the 97% that had been cracked. This is of course a very small number, and it is hard to interpret, but this might mean that our methods (specifically, building dictionaries from Wikipedia) were not used to crack the passwords. Regardless, the fact remains that our dictionaries allow us to crack around 5% of real-world databases, with pretty complex passwords, for a low amount of work.

## 2 Some interesting passwords

### 2.1 From the Korelogic database

```
perfect programmer syndrome // haltingproblem // SPARCstation 20 // Plain Old Telephone System //
MATH-MATIC or MATHMATIC // exercise, left as an //lots of MIPS but no I/O // getcashrightnow //
reincarnation, cycle of // eat flaming death // Gemfibrozil // lifematescanada // wall follower //
bestbadcreditpaydayloans // aneyeforaneyeatoothforatooth // jackofalltrades,masterofnone //
```

```
wherethereisawillthereisaway // afriendinneedisafriendindeed // worldchampionshipwrestling //
Do you speak English? // penisenlargementthatworks // All Your Base Are Belong To Us //
The quick brown fox jumps over the lazy dog. // Hey, what’s up? // Grapes of Wrath, The //
Who the hell are you? // Batman: The Animated Series // Fantastic Mr. Fox // I’m so sorry. //
Pirates of the Caribbean On Stranger Tides // What the hell are you talking about? //
itsonlyrockandrollbutilikeit // the cake is a lie // realfriendshelpyoumovebodies //
DROP THE WEAPON! // AllQuietontheWesternFront // putthatinyourpipeandsmokeit! //
ithinkweshouldseeotherpeople // idiaridellamotocicletta // breakonthroughtotheotherside //
MANYATRUEWORDISSPOKENINJEST // posttraumaticstresssyndrome // DICTATORSHIPOFTHEPROLETARIAT //
theforceisstrongwiththisone // panneauxsolairesthermiques // mockingjaybysuzannecollins //
solongandthanksforallthefish // schneewittchenunddiesiebenzwerge // Nonverbal communication //
wielkaorkiestraswiatecznejpomocy // saygoodnighttothebadguy // youarelikelytobeeatenbyagrue //
freeyourmindandyourasswillfollow // cashruleseverythingaroundme // YOUR PROPOSAL IS ACCEPTABLE. //
Use of deadly force is authorized // $(document).ready(function() // James T. Kirk //
WINNER_WINNER_CHICKEN_DINNER! // letthelittlechildrencometome // CHILD’S GARDEN OF VERSES, A //
Masque of the Red Death, The // les poules du couvent couvent // thebestthingsinceslicedbread //
Wikipedia, l’encyclopedie libre et gratuite // I could tell you but then I’d have to kill you //
Pa’s wijze lynx bezag vroom het fikse aquaduct // Cantami o diva del pelide Achille l’ira funesta
sesameouvretoi6 // WHAT THE-- // judge a man by his questions rather than by his answers
```

### 2.2 From other databases

- EHarmony: SINTIAUWHIAPLU // YOMISMAFUIMIRUTA (previously uncracked) ; 149162536496481100 // ANOTHERONEBITESTHEDUST // IDONTWANTTHISANYMORE // WHATTHEFUCKISGOINGON // FOREIGNEXCHANGESTUDENT // NOWISTHEWINTEROFOURDISCONTENT //CHANGEYOURPASSWORD // IWANTTOGETMARRIED
- Aha (previously uncracked): athousandsplendidsuns // bilawalbhuttozardari // brplvidyalaya // lefruitvert // HOMOPHOBIAISGAY // hppavilionze4900 // scrumpyjackcider // spinadipesce
- Gamigo (previously uncracked): alleaussermir // BackToFeature8 // honraatuspadres // elcaballodesantiago // pikachuetpichu // SpottedMarshFrog9 // Weltohnelicht // thazisogiamena2 // vocediperlablu7

## 3 Some interesting mnemonic-based passwords

### 3.1 From the Korelogic database

- "1lomtjjzictcttsdkcs": "Litwo! Ojczyzno moja! ..." (opening words of the classic Polish epic poem *Pan Tadeusz* by Adam Mickiewicz)
- "tamtihaehtadoiyp": "There are more things in heaven and earth, Horatio, than are dreamt of in your philosophy." (Shakespeare’s *Macbeth*)
- "fcpsitsgepgepgep": The acronym itself is the title of a song on the first album by the melodic punk band The Fall of Troy, and is thought to mean "Fuck Condoms Premarital Sex Is The Shit Get ’Em Pregnant Get ’Em Pregnant Get ’Em Pregnant"
- "wowowhiyhaynwa": "Walk on, walk on, with hope in your heart And you’ll never walk alone" (song "You’ll never walk alone")
- "isaaitaifteiknw": "I shot an arrow into the air, It fell to earth, I knew not where" (opening words of *The Arrow and The Song* by Henry Longfellow)

- "dngzhddddgigd7": "Denke nie gedacht zu haben, denn das Denken der Gedanken ist gedankenloses Denken!" (German tongue twister)
- "uuddlrlrababsS": "Up Up Down Down Left Right Left Right A B A B Select Start" (the "Konami Code", the most famous cheat code in gaming)
- "tbtitbtwtbtewb": "The best there is, the best there was, the best there ever will be" (catchphrase of the 1990s wrestler Bret "The Hitman" Hart)
- "Wcfavwfhpifar1": "Who can find a virtuous woman? For her price is far above rubies." (Book of Proverbs (from the Hebrew Bible), 31:10)
- "wmsteoopaaffwc": "We must secure the existence of our people and a future for White children." (the "fourteen words", a white nationalist slogan)
- "iejtmbdtiaeof": "In every job that must be done, there is an element of fun" (beginning of *A Spoonful of Sugar* from *Mary Poppins*).

### 3.2 From other databases

It is interesting to mention here that none of the passwords in this subsection had been cracked before.

- "whwhgtmgathn": "Whatever happens we have got // the Maxim gun and they have not" (poem *The Modern Traveller* by Hilaire Belloc) ; **Gamigo** database
- "aiwsittdrcau": "All I wanna say is that they don't really care about us" (song "They don't care about us" by Michael Jackson) ; **Aha** database
- "wmkahemfh" : "Wenn man keine Ahnung hat einfach mal Fresse halten" (famous quip by comedian Dieter Nuhr, translates to "If you have no idea, just keep your face shut"?) ; **Gamigo**
- "LDWMJOMTTKTP": "Last dance with Mary Jane, one more time to kill the pain" (Tom Petty and the Heartbreakers song) ; **Eharmony**
- "HTHFATPASIHSTG" (this is an expression in the same style as "as far as i'm concerned" and "your mileage may vary", but I don't know which one) ; **Eharmony**
- "NVSTFTSAF" ; **Eharmony**
- "L,die,aHf!" ; **Gamigo**
- "iygcbtmanyc" ; **Gamigo**
- "eindsddwiwsi" ; **Gamigo**
- "geepfddgztw" ; **Gamigo**
- "RfIudMiIUeSz" ; **Gamigo**

## 4 Best passphrase-mangling rules

Out of the 94 rules considered, which ones are best? We see how much they can crack out of a random section of 3 million hashes from the Korelogic database.

| Rule | Pwd cracked |
|---|---|
| Del spaces, lowercase | 13,736 |
| Del spaces, append digit | 12,769 |
| Del spaces+punct, append digit | 8,460 |
| Del spaces, append digit, lowercase | 7,098 |
| Del spaces | 6,949 |
| Del spaces, append digit, uppercase | 6,563 |
| Lowercase | 5,602 |
| Append digit | 5,445 |
| Del spaces+symbol, append digit | 4,203 |
| Del punct, append digit | 3,940 |