

Hunting For Passwords Or Putting An End To The Arms Race

Sébastien Raveau

Passwords^{^12}, Oslo, Norway

December 3rd 2012

Disclaimer

- I am here representing neither my (professional) work nor my employer.

Me, Myself And I

- wikipedia-wordlist-sraveau-20090325.txt.bz2
- <http://blog.sebastien.raveau.name/>
- Idling on IRC, notably as @Kryczek in Freenode's ##security and EFNet's #asm
- Occasional contributions to OSS: TCPdump, TCPslice, Metasploit, BackTrack, Squid, OpenVPN, Iodine, PingTunnel, Debian Live, MPlayer, KHTML, maybe others

<http://twitter.com/sraveau>



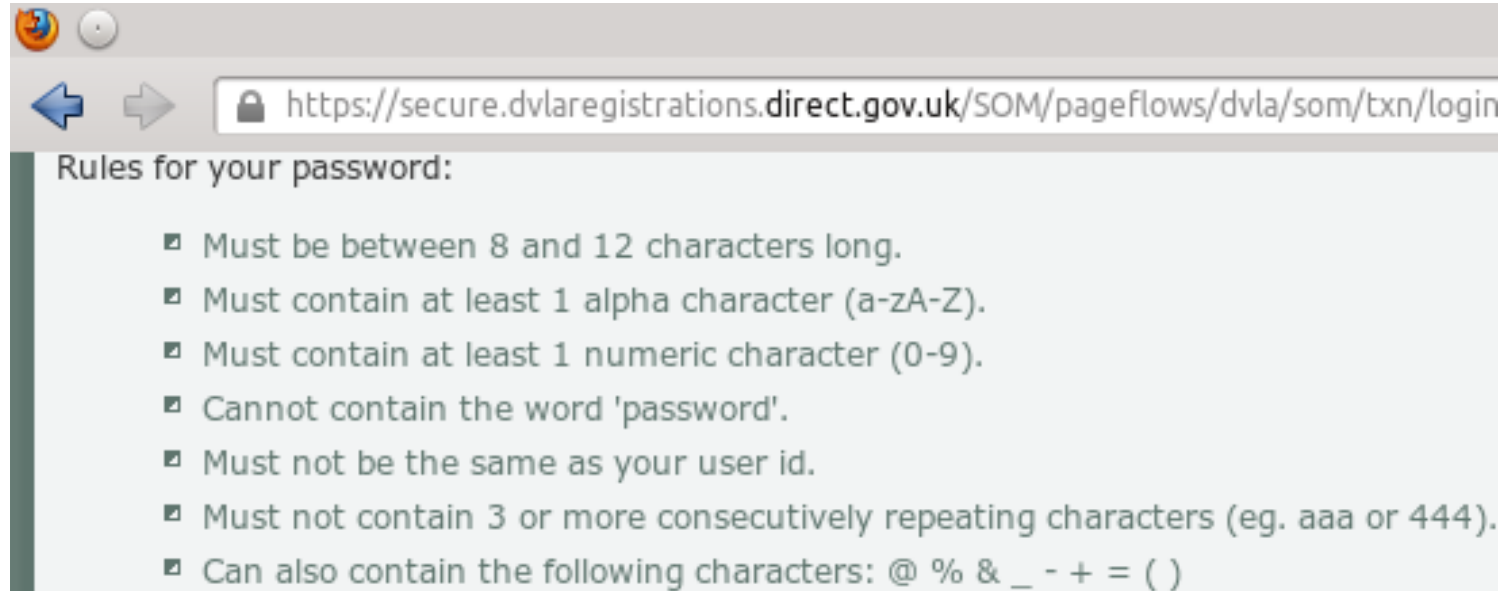
This is where the hacking happens,
someone uses telnet to metasploit the
RPC service using overflow bytes and
bad passwords to connect the buffer

“[Pass]words are very unnecessary, they can only do harm”

Depeche Mode – Enjoy The Silence

In terms of authentication, are we really going in the right direction?

So-called strong password policies can do more harm than good



- Can't use my usual per-domain password generation scheme; can't use something I would remember like *lol@drivingontheleft*
- Ok *Password1* won't work but *LetMeIn1* will

A funny? joke on the Internet



- During an audit it was found that a blonde was using the following password:
MickeyMinniePlutoHueyLouieDeweyDonaldGoofySacramento
- When asked why she had such a long password she rolled her eyes and said:
“Hello! It has to be at least 8 characters long and include at least one capital.”

The UIO portal

- A password must be at least 8 characters long and contain characters from at least 3 of the numbers, lowercase, uppercase & special categories
- A password must not contain æ, ø or å; contain words found in a dictionary or resemble one of your previous set password
- “Bad password: For a password to be valid **the first 8 characters** must be from at least three of these four character groups: Uppercase letters, lowercase letters, numbers and special characters.”
- “Changes will be applied within 4 hours.”

Password expiry policies can do more harm than good

- As people run out of personal passwords they resort to much less confidential information like *December2012* or *LatitudeE6410*
- Requiring people to change their password frequently on several different systems pushes them to use the same one everywhere
- When people start struggling to remember they start writing passwords down

...on post-its



(on the monitor, under the keyboard, under the phone, under the mouse-pad, under the desk, in a drawer, etc)

...in notebooks and now dedicated password organizers



...on the wall for everyone to see



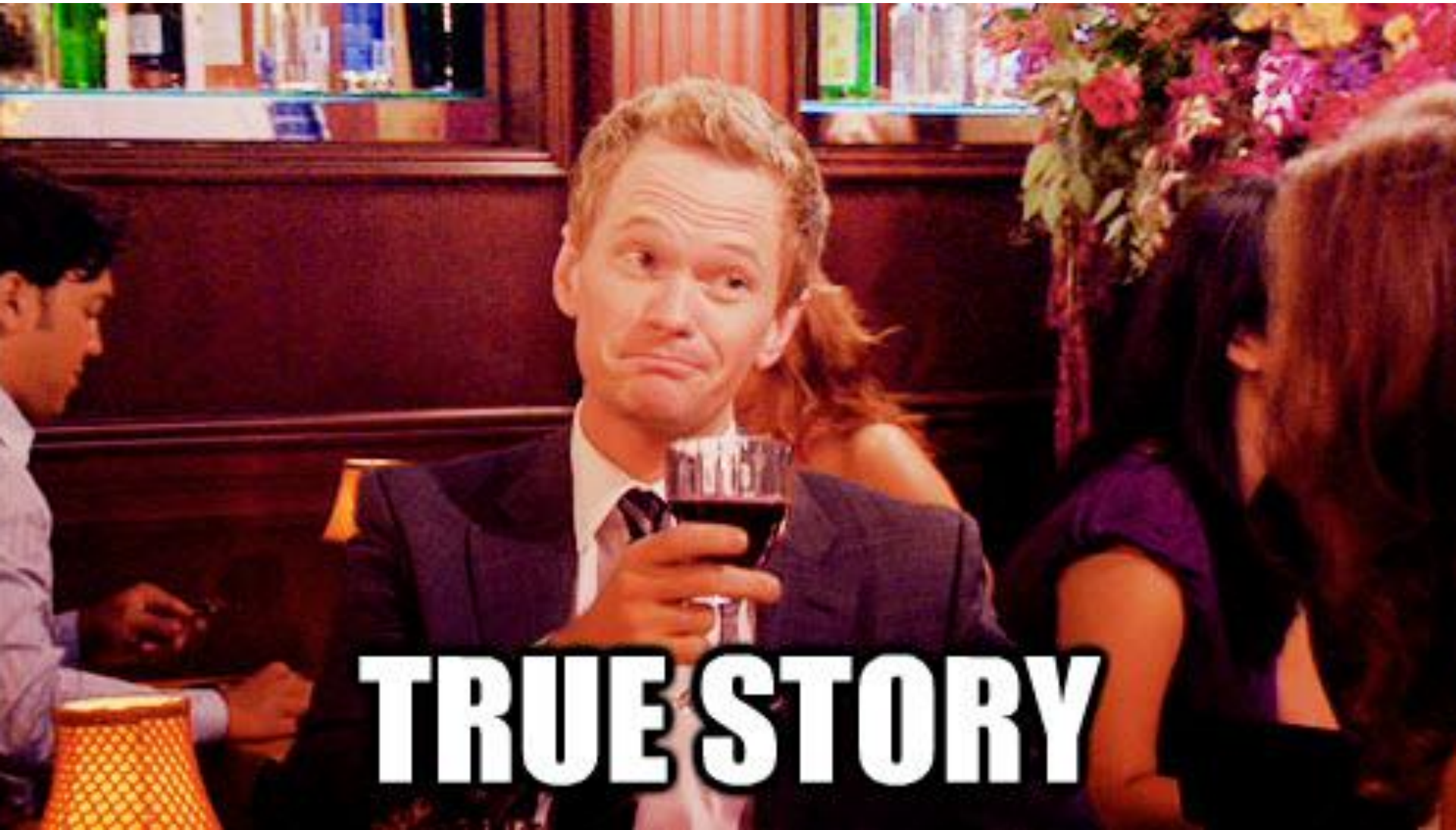
...wall (Interview? No problem!)



...wall (Photo shoot? No problem!)



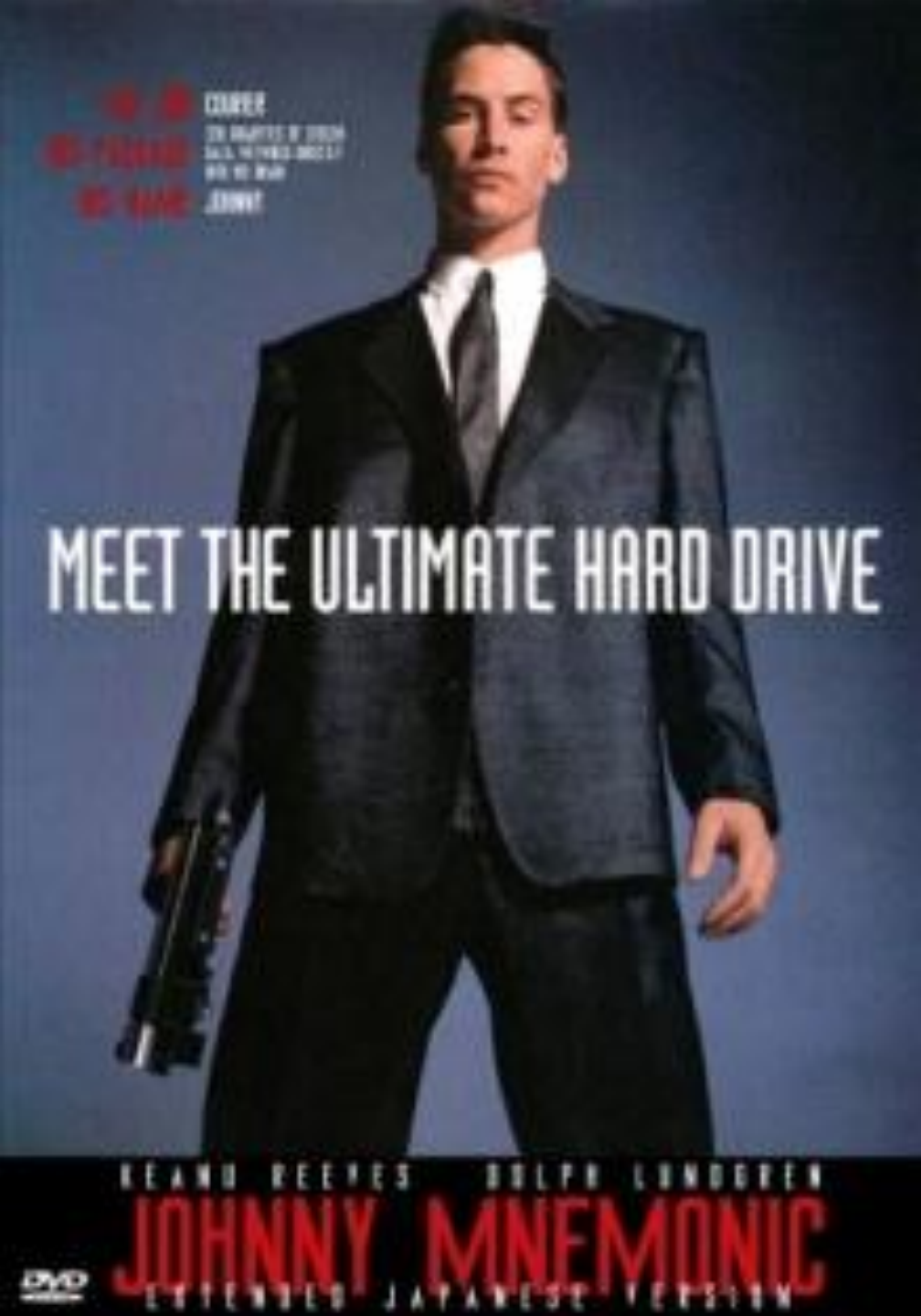
...on disk or worse: in shared folders
with read & write access for everyone



“Why need I volumes if one [pass]word suffice?”

Ralph Waldo Emerson

**Dropping these requirements does not
make for good passwords either**



Conflict of interest:
the human brain
cannot be used as
reliable storage
(yet?) so most if
not all people
prefer to have to
remember only
one password and
one that is as
simple as possible

Human nature

- When asked to choose a password people tend to look around
- Brands in the field of vision and other names in the news/culture seem very inspiring
- Most if not all password filters have absolutely no problem with non-dictionary words that could easily be guessed like *Alienware*, *Blink182*, *Numb3rs*, *30Rock*, *Left4Dead*, etc

Solution?

- We need a wordlist of every brand, every name, every word in any language ever
- The Internet might contain all of those (anyone here working at Google?) but with reasonable resources the contents of the Wikimedia websites: Wikipedia, Wikibooks, Wikinews, Wikiquote, Wikisource, Wikiversity and Wiktionary is a good start

Problem #1: Burmese

လက်ပံတောင်းတောင်သပိတ် အရေးအခင်း

လက်ပံတောင်းတောင် သပိတ်အရေးအခင်းသည် လက်ပံတောင်း၊ ဆားလင်းကြီးမြို့၊ မုံရွာတဘက်ကမ်းတွင်တည်ရှိသည့် ကြေးနီစီမံကိန်းအား ရပ်ဆိုင်းရေးအတွက် ဒေသခံ ရွာသူရွာသားများမှ ဆန္ဒပြသပိတ်မှောက်ခဲ့ကြခြင်းဖြစ်သည်။ ထိုကြေးနီစီမံကိန်းအား ကန့်ကွက်ရန် စတင်ဆန္ဒပြခဲ့ကြသူများမှာ ရန်ကုန်ပြည်သူ့ အကျိုးဆောင် ကွန်ယက်မှ လယ်သမားအရေးလုပ်ဆောင်သူ ကိုဝေဠု၊ ဝက်မွေးရွာသူဖြစ်သည့် မသွဲ့သွဲ့ဝင်း၊ မအေးနက် နှင့် မဖြူဖြူဝင်းတို့သည်။ မုံရွာ ဆုတောင်းပြည့် ဘုရား၌ ဝတ်ပြုဆုတောင်းခဲ့ရာမှ ဩဂုတ်လ ၃၀ရက်နေ့တွင် အာဏာပိုင်တို့၏ ဖမ်းဆီးခြင်းကို ခံခဲ့ရသည်။ ၁၄ရက်မျှ အဖမ်းခံရပြီးနောက်ပိုင်း ၎င်းတို့အားလုံး ပြန်လည်လွတ်မြောက်ခဲ့သည်။^[၁] ၎င်းတို့ပြန်လွတ်မီ ၁ရက်အလိုတွင် ၈၈ မျိုးဆက်ကျောင်းသား ခေါင်းဆောင်များနှင့် အစိုးရ အဖွဲ့များအကြား ဆွေးနွေးညှိနှိုင်းမှုများရှိခဲ့ပြီး လိုက်လျောမှုတချို့လည်း ရရှိခဲ့သည်။ တောင်းဆိုမှု သုံးချက်တွင် ဖမ်းဆီးခံရသူများ ပြန်လည်လွတ်ပေးရေး၊ ဆန္ဒပြမည့်သူများကို ဖမ်းဆီးခြင်းမပြုလုပ်ရန်၊ ကြေးနီစီမံကိန်းအား ရပ်တန့်ထားရန် တောင်းဆိုခဲ့သော်လည်း၊ အာဏာပိုင်တို့မှ ဒုတိယအချက်ကို လိုက်လျောခဲ့ပြီး၊ ဆန္ဒပြမည့်သူများကို ဖမ်းဆီးခြင်း ထပ်မလုပ်ရန် ကတိပေးခဲ့သည်။

တောင်းဆိုခဲ့သည့် ပထမအချက်သည်၊ အာဏာပိုင်တို့မှ တရားဥပဒေအရ အရေးယူခြင်းဖြစ်သောကြောင့် ဥပဒေအကြောင်းအရသာ ပြန်လည်လွတ်ပေးမည်ဟု ဖြေကြားခဲ့သည်။^[၂]

- မာတိကာ** [၄က်]
- ၁ ဦးပိုင်ကုမ္ပဏီ နှင့် ဝမ်ပေါင်
 - ၂ ရန်ကုန်၌ ဆန္ဒပြ
 - ၃ ဆန္ဒပြမှု အရှိန်မြှင့်
 - ၄ ကိုးကား

ဦးပိုင်ကုမ္ပဏီ နှင့် ဝမ်ပေါင်

[ပြင်ဆင်ရန်]

ထိုစီမံကိန်းအား ပူးတွဲလုပ်ဆောင်နေသည့် ဦးပိုင်ကုမ္ပဏီ နှင့် ဝမ်ပေါင်ကုမ္ပဏီတို့မှ လက်ရှိဖြစ်ပျက်နေသည့် သဘာဝ ပါတ်ဝန်းကျင် ပျက်စီးမှုများသည် ၎င်းတို့၏ စီမံကိန်းများကြောင့် မဟုတ်ဟုဆိုကာ ဂရုစိုက်ရေးအတွက် တောင်းဆိုထားသော်လည်း သတင်းစာရှင်းလင်းပွဲ ပြုလုပ်၍ ငြင်းဆိုခဲ့သည်။ ထိုဒေသရှိ စပယ်တောင် နှင့် ကြေးစင်တောင်များ ပျောက်သွားခဲ့သော်လည်း၊ ကုမ္ပဏီမှ တောင်များကို ပြန်လည်ပုံဖော်၍ သစ်ပင်များပြန်လည်စိုက်ပျိုးပေးမည်ဖြစ်ကြောင်းလည်း ဖြေကြားခဲ့သည်။^[၃]

Problem #1: Chinese, Classical Chinese, Simplified Chinese, Gan, Wu and Cantonese

人口

[编辑]

黃巾之亂后，中原地區發生天災饑荒，例如：「建寧三年春正月，河內人婦食夫，河南人夫食婦」等紀錄。[董卓](#)掌權後，放縱士兵淫略婦女，剽虜資物。在面對關東軍聯合討伐下，竟然「盡徙洛陽人數百萬口於長安，悉燒宮廟官府居家，二百里內無復孑遺」，以至於民怨載道，人口數大減。[曹操](#)征徐州時，「凡坑殺男女數十萬人，雞犬無餘，泗水為之不流，自是五縣城保，無復行跡」。 [李傕](#)等在關中，「時三輔民尚數十萬戶，傕等放兵劫略，攻剽城邑，人民飢困，二年間相啖食略盡」。益州的[劉焉](#)、[劉璋](#)及荆州的[劉表](#)鎮壓叛亂，揚州因為[孫策](#)等人的戰爭，使得人口數都減少。

當時的人民朝三個方向流動：由關中西遷至涼州或是南遷至益州、沿漢水遷移至荊州，各約十萬戶。由中原地區往東北遷移至冀州或幽州，再遷至遼東。[鮮卑](#)和[烏桓](#)也因為這波流民而壯大。最後也是最大一股，是由中原地區遷移至徐州彭城，再南遷至江南地區。當時「是時四方賢士大夫避地江南者甚眾」，孫吳立國的基礎即建立在此上。例如：[魯肅](#)、[諸葛瑾](#)、[呂蒙](#)、[張昭](#)及[徐盛](#)等人就是此次南渡的中原士族之一。

自三國鼎立局勢漸漸形成後，人民轉而因統治者或戰爭而被迫遷移。[曹操](#)攻擊張魯時及攻下後，共遷部份的川東漢中居民入關中。曹丕建都洛陽後，遷冀州五万户士家以實河南。魏灭蜀后遷蜀人三万家至洛阳和关中。劉備領有益州，多次迁民于成都平原。諸葛亮第一次北伐失敗後，也遷隴西居民以實漢中。[孫權](#)在早期即擊敗江夏太守黃祖，虜掠男女數萬口。他建國後為了提昇人口數，平定山越並以其「贏者充戶，強者補兵」，並且騷擾淮南來獲得人口。

以下表格可知人口銳減趨勢。由東漢晚期到西晉統一全國，雖然時間僅隔125年，但人口只有東漢人口峰值的35.3%。至此戶口一蹶不起，至到隋文帝在位時方漸復甦。另外值得注意的是人口高度的軍事化，當時三國控制的人口還有兵戶、吏戶、屯田戶等。例如曹操早在創建時期即推行屯田制。蜀漢人口雖只有九十萬，但是却有十萬多的軍隊^[26]，佔總人口十分之一。而屯田戶數量之大，对当时社会经济的恢复和发展起着决定性作用^[27]。

Problem #1: Dzongkha

ལྷ་འཕོང་གི་ལྷ་ཁྱེད་པ།

[ལྷ་ཁྱེད་པ།]

- གོང་མ་ ལོ་རྒྱུན་དབང་ལྷག་མཚོག་ ཡལ་འཇིགས་མེད་དབང་རྒྱལ་དང་ དུམ་ཨ་ལེམ་ བརྒྱ་ཚོས་སྤྱིད་གཉིས་ཀྱི་སྤྲུལ་ལུ་ ༡༥༦༢ ལུ་ ལྷ་ཁྱེད་པ་རྒྱལ། ཡལ་འཇིགས་མེད་རྣམ་རྒྱལ་མཚོག་ གཏུང་དཀར་ཚོས་རྗེ་ཡི་ལ་དཔོན་པོ་དབང་རྒྱལ་དང་ བསོད་ནམས་དཔལ་འཛོམས་གཉིས་ཀྱི་སྤྲུལ་ཨིན། དོ་རྗེ་དང་ གཏུང་དཀར་རྒྱལ་མཚོན་ དེ་ལས་ ཚོ་རྒྱུ་ལེ་མ་དང་ གཡུ་རྫོང་རྩོམ་གྱི་རྒྱུ་ཚ་ ཨིན་མ་དང་ གཏུང་དཀར་རྒྱལ་མཚོན་གྱིས་ རྒྱང་གསལ་དཔོན་རྫོབ་ཀྱི་གོ་གནས་བཞེས་རྒྱལ།

དུམ་བརྒྱ་ཚོས་སྤྱིད་དེ་ གཏུང་ལོང་ཚོས་རྗེ་ ལོ་རྒྱུན་ལྷ་ཚོགས་ཀྱི་ སྤྲུལ་ཨིན་མ་དང་ ལོ་རྒྱུན་ལྷ་ཚོགས་དེ་ བད་སྤྱིད་གཏུང་ས་རྒྱལ་ སམ་ ཀྱུན་བཟང་བརྒྱན་པའི་ཉི་མ་དང་ རྒྱང་གསལ་དཔོན་ རྫོབ་པ་དབང་འཛོམས་གཉིས་ཀྱི་རྒྱུ་རྩ་ཨིན། ལོ་རྒྱུན་ལྷ་ཚོགས་ཀྱིས་ རྒྱང་གསལ་དཔོན་རྫོབ་ཀྱི་གོ་གནས་ཡང་བཞེས་རྒྱལ།

གོང་ སའོ་རྒྱུན་དབང་ལྷག་མཚོག་ལུ་རྒྱ་མཚོད་གཉིས་ཡོད་མི་ནང་ལས་ ལྷན་ལས་ རྫོབ་ས་རྒྱུས་ཀྱིས་ དབང་འབྲུལ་མོ་བྱང་རྫོང་དཔོན་དང་ རྫོང་དཔོན་རྫོབ་ཀྱི་གོ་གནས་བཞེས་ཡོད་པ་དང་ ཡེ་ཤེས་ ཚོས་རྫོང་དེ་ ལྷ་དཀར་རྫོང་དཔོན་ འཚོ་མེད་རྗེ་དང་གཅིག་ཁར་གཉིན་རྫོང་འབབ་རྒྱལ།

གོང་ སའོ་རྒྱུན་དབང་ལྷག་མཚོག་ རྒྱང་གསལ་དཔོན་རྫོབ་ བརྒྱ་བརྒྱན་འཛོམས་ཀྱི་སྤྲུལ་ཨིན་མེད་དང་ ལྷ་ཁྱེད་པོ་ལེ་ལས་ ཨིན་མི་ ཀྱུན་བཟང་འཇིགས་ལས་ཀྱི་སྤྲུལ་ཨོ་ ཨ་ལེ་ ལྷ་མོ་ གཉིས་ དང་གཅིག་ཁར་གཉིན་རྫོང་མཚོད་རྒྱལ། ཨ་ལེ་རྗེ་ཚེན་ལས་ སྤྲུལ་ཨོ་ དཔལ་རྫོང་དང་དབང་ས་འཛོམས་སྤུ་འབྲུང་ས་ཡོད་པ་དང་ ཨ་ལེ་ ལྷ་མོ་ལས་ སྤྲུལ་ཨོ་ དབང་མོ་ སྤྲུལ་འབྲུང་མེད་རྗེ་དང་ ཀམ་འཇིགས་ལས་ དེ་ལས་ འཇིགས་མེད་དབང་ལྷག་ཚ་སྤུ་འབྲུང་ས་རྒྱལ།

- འབྲུག་རྒྱལ་པོ་ འཇིགས་མེད་དབང་ལྷག་མཚོག་ ༡༧༠༥ ལུ་ ཡེ་ཤེས་ལུ་ ཡལ་ལོ་རྒྱུན་དབང་ལྷག་དང་ དུམ་ཨ་ལེམ་གྱི་སྤྲུལ་ལུ་ ལྷ་ཁྱེད་པ་རྒྱལ། མི་དབང་མཚོག་ ལྷ་སྤྱད་ལལ་ དོ་ དག་པོས་ འཇིགས་དབང་ས་ཀྱི་སྤྲུལ་ཨོ་ ཨ་ལེ་ ལྷ་ཚོགས་ཚོས་རྫོང་དང་ ཨ་ལེ་ བརྒྱ་བདེ་ཚེན་དང་གཅིག་ཁར་ གཉིན་རྫོང་མཚོད་གནང་རྒྱལ། ཨ་ལེ་ ལྷ་ཚོགས་ཚོས་རྫོང་ལས་ སྤྲུལ་ འཇིགས་མེད་རྗེ་དབང་ལྷག་དང་ ཨ་ལེ་ བརྒྱ་བདེ་ཚེན་ལས་ སྤྲུལ་ རྣམ་རྒྱལ་དབང་ལྷག་དང་ སྤྲུལ་ཨོ་ ཚོས་སྤྱིད་དང་ བདེ་སྤྱིད་དབང་ས་འཛོམས་ དེ་ལས་ བརྒྱ་ཚོས་རྫོང་རྩོམ་སྤུ་འབྲུང་ས་རྒྱལ།

- འབྲུག་རྒྱལ་པོ་ འཇིགས་མེད་རྗེ་དབང་ལྷག་མཚོག་ ༡༧༢༥ ལུ་ ཡལ་འཇིགས་མེད་དབང་ལྷག་དང་ དུམ་ཨ་ལེམ་ལྷ་ཚོགས་ཚོས་རྫོང་གཉིས་ཀྱི་སྤྲུལ་ལུ་ ལྷ་ཁྱེད་པ་རྒྱལ། མི་དབང་ མཚོག་ རྒྱང་གསལ་བསོད་ནམས་རྫོབ་ས་རྒྱུས་དང་ སི་གི་མ་ལས་ ཨ་ལེ་ ཚོས་དབྱིད་ས་དབང་མོ་གཉིས་ཀྱི་སྤྲུལ་ཨོ་ ཨ་ལེ་ བརྒྱལ་བཟང་ཚོས་རྫོང་དང་གཅིག་ཁར་གཉིན་རྫོང་མཚོད་རྒྱལ། ཨ་ལེ་ བརྒྱལ་བཟང་ལས་ སྤྲུལ་ འཇིགས་མེད་མེད་གོ་དབང་ལྷག་དང་ ཨ་ལེ་ བསོད་ནམས་ཚོས་རྫོང་དང་ བདེ་ཚེན་དབང་མོ་ བརྒྱལ་བཟང་དབང་མོ་དང་ད བརྒྱ་བརྒྱན་ཚོ་འབྲུང་ས་རྒྱལ།

- འབྲུག་རྒྱལ་བཞི་པ་ འཇིགས་མེད་མེད་གོ་དབང་ལྷག་མཚོག་ ༡༧༥༥ ལུ་ ཡལ་འཇིགས་མེད་རྗེ་དབང་ལྷག་དང་ དུམ་ཨ་ལེམ་ བརྒྱལ་བཟང་ཚོས་རྫོང་གཉིས་ཀྱི་སྤྲུལ་ལུ་ ལྷ་

Problem #1: Japanese

化学的性質 [編集]

ベリリウムの単体は還元性が非常に強く、その標準酸化還元電位 E_0 は -1.85 V である^[12]。この標準電位の値はイオン化傾向においてアルミニウムの上に位置しているため大きな化学活性が期待されるが、実際には表面が酸化物の膜（酸化被膜）に覆われて不動態化するため高温に熱した状態でさえも空気や水と反応しない。しかしながら、一旦点火すれば輝きながら燃焼して酸化ベリリウムと窒化ベリリウムの混合物が形成される^[13]。

ベリリウムは通常、表面に酸化被膜を形成しているため酸に対しての強い耐性を示すが、酸化被膜を取り除いた純粋なベリリウムでは塩酸や希硫酸のような酸化力を持たない酸に対しては容易に溶解する。硝酸のような酸化力を有する酸に対してはゆっくりとしか溶解しない。また、強アルカリに対してはオキソ酸イオンであるベリリウム酸イオン ($\text{Be}(\text{OH})_4^{2-}$) を形成して水素ガスを発生させながら溶解する。このような酸やアルカリに対する性質はアルミニウムと類似している^[14]。ベリリウムは水とも水素を発生させながら反応するが、水との反応によって生じる水酸化ベリリウムは水に対する溶解度が低く金属表面に被膜を形成するため、金属表面のベリリウムが反応しきればそれ以上反応は進行しない^[15]。



ベリリウム原子の電子配置は $[\text{He}] 2s^2$ である。ベリリウムはその原子半径の小ささに対してイオン化エネルギーが大きいいため電荷を完全に分離することは難しく、そのためベリリウムの化合物は共有結合性を有している^[16]。第2周期元素は原子量が大きくなるにしたがってイオン化エネルギーも増大する法則が見られるがベリリウムはその法則から外れており、より原子量の大きなホウ素よりもイオン化エネルギーが大きい。これは、ベリリウムの最外殻電子が2s軌道にあり、ホウ素の最外殻電子は2p軌道にあることに起因している。2p軌道の電子は内殻に存在するs軌道の電子によって遮蔽効果（有効核電荷も参照）を受けるため、2p軌道に存在する最外殻電子のイオン化エネルギーが低下する。一方で2s軌道の電子は遮蔽効果を受けないため、相対的に2p軌道の電子よりもイオン化エネルギーが大きくなり、これによってベリリウムとホウ素の間でイオン化エネルギーの大きさの逆転が生じる^[17]。

Problem #1: Korean

공연 활동

[편집]

- 싸이는 2012년 7월 15일 SBS <인기가요>에서 <강남 스타일>을 선보이며 컴백했다.^[14] 2012년 8월 15일에는 서울 잠실종합운동장 보조경기장에서 싸이의 썸머스탠드 월씬 THE 홈백쇼에서 <강남스타일>을 세트리스트 중 하나로 선정했고, 8월 25일 MBC <음악중심>을 통해 콘서트 실황이 방송됐다.^[15]
- 특히 싸이는 이 노래를 통해 미국으로도 진출했는데, 2012년 8월 23일 VH1의 <빅 모닝 버즈 라이브>에 출연해 인터뷰와 말춤을 선보였다.^[16] 이후 대한민국 활동을 정리하는대로 2012년 9월 중으로 다시 미국에 방문한다고 밝혔다.^[17]
- 2012년 9월 6일에는 로스앤젤레스 스테이플 센터에서 열린 2012 MTV 비디오 뮤직 어워드에 케빈 하트와 시상자로 나섰다. 싸이는 시상식에서 말춤을 선보였고, "일단 기분 너무 좋고 너무 행복합니다. 이 무대에서 한 번쯤은 한국말을 해보고 싶습니다. 죽이지?"라며 한국어로 말하기도 했다.^[18]
- 2012년 9월 11일에는 <엘렌 드제네러스 쇼>에 게스트로 출연해 브리트니 스피어스와 사이먼 코웰에게 말춤을 알려 줬고, 당시 3%의 시청률이 나오면서 2003년 이래 최고 시청률을 경신했다.^[19] 2012년 9월 14일에는 NBC의 <투데이 쇼>에 출연해 <강남 스타일>을 선보였다.^[20]
- 한편 싸이는 미국 빌보드 차트 1위를 달성했을 때 '사람들이 많이 모일 수 있는 장소에서 상의를 탈의한 채 말춤을 추겠다'고 약속^[21]한 바가 있었으나 빌보드 차트 순위 발표를 며칠 남겨두고 이를 '순위에 상관없이 성원에 대한 보답의 뜻으로 많은 사람들이 관람할 수 있는 장소에서 무료 공연을 실시하겠다'고 약속을 수정하였다. 이에 따라 2012년 10월 4일 밤 10시에 서울 광장에서 약 1시간 30분 동안의 무료 공연을 전격 시행하였다. 이 공연을 시작하기 몇 시간 전에 발표된 빌보드 차트 순위에서는 1위를 달성하지 못했으며 2주째 2위에 머물렀다.
- 2012년 10월 4일 서울 광장에서 펼쳐진 무료 공연은 유튜브를 통해 실시간 스트리밍으로 중계되었다. 이날 동시 접속수는 10만 명에 육박하였으며 이로 인해 스트리밍이 원활하지 못했다. 이날 유튜브를 통해 스트리밍된 전체 영상은 다시 볼 수 있도록 싸이의 공식 ID인 'officialpsy'의 이름으로 올려져 있었으나 무대 위에서 소주를 병째로 마시는 장면이 여과없이 노출됨에 따라 현재는 노

Problem #1: Lao

ນິກາຍເຖລະວາດ

ເຖລະວາດ, sthaviravada 'ສະຖະວິລິວາດ ໂດຍສັບແປວ່າ "ຕາມແນວທາງຂອງພະເຖລະ" ເປັນຊື່ຂອງ **ນິກາຍ** ທີ່ເກົ່າແກ່ທີ່ສຸດໃນ **ສາດສະໜາພຸດ** ໃນພຸດທະສາສະໜາຝ່າຍມະຫາຍານ ຮຽກນິກາຍນີ້ວ່າ **ຫິນະຍານ** ຫລື **ຫິນະຍານ**

ນິກາຍເຖລະວາດ ເປັນນິກາຍຫລັກ ທີ່ໄດ້ຮັບການນັບຖືໃນ **ປະເທດສີລັງກາ** (ປະມານ 70% ຂອງປະຊາກອນທັງໝົດ ແລະ ປະເທດໃນແຜ່ນດິນ **ອາຊີຕາເວັນອອກສຽງໃຕ້** ໄດ້ແກ່ **ໄທ ກຳປູເຈຍ ລາວ ແລະ ມຽນມາ** ນິກາຍເຖລະວາດ ໄດ້ຮັບການນັບຖືເປັນສ່ວນນ້ອຍໃນ **ປະເທດຈີນ ແລະ ຫວຽດນາມ** ໂດຍສະເພາະໃນ **ແຂວງຢູນນານ ເນປານ ບັງຄະລາເດດ** ທີ່ **ເຂດຈິດຕະກອງ ຫວຽດນາມ** ທາງຕອນໃຕ້ໃກ້ຊາຍແດນ ກຳປູເຈຍ **ມາເລເຊຍ** ມີນັບຖືທາງຕອນເໜືອຂອງປະເທດ ມີສາສະນິກະຊົນສ່ວນໃຫຍ່ເປັນເຊື້ອສາຍ **ໄທ ແລະ ສິງຫິນ** ຕົວເລກຜູ້ນັບຖືສາສະໜາພຸດ ນິກາຍເຖລະວາດມີຢູ່ປະມານ 100 ລ້ານຄົນ. ສຳລັບປະເທດລາວ ມີຜູ້ນັບຖືສາສະໜາພຸດ ປະມານ 80% ຂອງຈຳນວນປະຊາກອນທັງໝົດ.

ຄວາມເປັນມາຂອງນິກາຍເຖລະວາດ

[ດັດແກ້]

ຫລັງຈາກ **ພະພຸດທະເຈົ້າ** ສະເດັດດັບຂັນປະລິນິບພານໄດ້ 3 ເດືອນ ພະສາວົກຜູ້ໄດ້ເຄຍໄດ້ສະດັບຄຳສັ່ງສອນຂອງພະອົງຈຳນວນ 500 ຮູບ ກໍປະຊຸມເຮັດ **ສັງຄາຍະນາ** ເທື່ອທຳອິດ ທີ່ **ຖ້ຳສັດຕະບັນຄູຫາ** ໃກ້ເມືອງ **ລາຊະຄຶ** ແຄວ້ນ **ມະຄົດ** ໃຊ້ເວລາສອບທານຢູ່ 7 ເດືອນ ຈຶ່ງປະມວນຄຳສອນຂອງພະພຸດທະເຈົ້າໄດ້ສຳເລັດເປັນເທື່ອທຳອິດ ນັບເປັນບໍ່ເກີດຂອງຄຳພີ **ພະໂຕຣປິດົກ** ຄຳສອນທີ່ລົງມະຕິກັນໄວ້ໃນຄັ້ງ ປະຖົມສັງຄາຍະນາ ແລະ ໄດ້ນັບຖືກັນສືບມາ ຮຽກວ່າ **ເຖລະວາດ** ແປວ່າ ຄຳສອນທີ່ວາງໄວ້ເປັນຫລັກການໂດຍພະເຖລະ ຄຳວ່າ **ເຖລະ** ໃນທີ່ນີ້ ໝາຍເຖິງ ພະເຖລະຜູ້ປະຊຸມເຮັດສັງຄາຍະນາເທື່ອແຮກ ແລະ ພະພຸດທະສາສະໜາຊຶ່ງຖືຕາມຫລັກທີ່ໄດ້ສັງຄາຍະນາເທື່ອແຮກດັ່ງກ່າວ ຮຽກວ່າ **ນິກາຍເຖລະວາດ** ອັນໝາຍເຖິງ ຄະນະສົງກຸ່ມທີ່ຍຶດຄຳສັ່ງສອນຂອງພະພຸດທະເຈົ້າ ທັງຖ້ອຍຄຳ ແລະ ເນື້ອຄວາມທີ່ທ່ານສັງຄາຍະນາໄວ້ໂດຍເຄັ່ງຄັດ ຕະຫລອດຈົນຮັກສາ ແມ່ນແຕ່ຕົວພາສາດັ້ງເດີມຄື **ພາສາບາລີ**



ນິກາຍຍ່ອຍ

[ດັດແກ້]

ນິກາຍເຖລະວາດ ຍັງມີນິກາຍທີ່ແບ່ງຍ່ອຍອອກໄປອີກຈາກເດີມ ມີຄວາມແຕກຕ່າງກັນນຳຕາມທ້ອງຖິ່ນນັ້ນໆ ໂດຍນິກາຍຍ່ອຍຂອງເຖລະວາດມີຢູ່ ໄດ້ແກ່:



Problem #1: Thai

การก่อตัว

[แก้]

ปี ค.ศ. 1802 เฮนริก โอลเบอร์ เสนอกับวิลเลียม เฮอร์เชล ว่า แถบใหญ่ที่น่าจะเกิดจากดาวเคราะห์ดวงหนึ่งที่ระเบิดเป็นผุยผงด้วยสาเหตุใดสาเหตุหนึ่ง^[17] แต่เมื่อเวลาผ่านไป สมมุติฐานนี้ก็ตกไป เพราะไม่สมเหตุผลที่จะมีพลังงานจำนวนมากในการกระทำให้เกิดเหตุการณ์เช่นนั้น รวมทั้งปริมาณมวลรวมของวัตถุในแถบดาวเคราะห์น้อยก็น้อยมาก เพียงเสี้ยวเล็กๆ ส่วนหนึ่งของดวงจันทร์ของโลกเท่านั้น นอกจากนั้นยังมีข้อมูลด้านเคมีที่แสดงให้เห็นว่า ดาวเคราะห์น้อยแต่ละดวงมีคุณสมบัติทางเคมีที่แตกต่างกันมากจนเกินจะอธิบายได้ว่ามันเกิดมาจากดาวเคราะห์ดวงเดียวกัน^[18] ปัจจุบันนักวิทยาศาสตร์ส่วนใหญ่เชื่อว่าชิ้นส่วนดาวเคราะห์น้อยไม่ได้เกิดจากดาวเคราะห์ดวงเดียวกัน แต่มันไม่เคยรวมตัวเป็นดาวเคราะห์ได้สำเร็จมากกว่า

ตามปกติแล้ว การกำเนิดของดาวเคราะห์ในระบบสุริยะเชื่อกันว่าเกิดขึ้นจากกระบวนการที่คล้ายคลึงกับ**เนบิวลา** กล่าวคือมีกลุ่มเมฆฝุ่นและ**ก๊าซ** ในห้วงอวกาศที่มารวมตัวกันเนื่องจากอิทธิพลของ**แรงโน้มถ่วง** ทำให้เกิดเป็นจานหมุนประกอบด้วยวัตถุสสารที่อัดแน่นจนกลายเป็น**ดวงอาทิตย์** และ**ดาวเคราะห์**^[19] ในช่วงไม่กี่ล้านปีแรกของประวัติศาสตร์ระบบสุริยะ กระบวนการอัดแน่นนี้ทำให้ชิ้นส่วนฝุ่นหินเล็กๆ รวมตัวกันและเพิ่มขนาดขึ้นเรื่อยๆ เมื่อมีการรวมตัวกันจนได้ขนาดมวลมากพอ มันจะสามารถดึงดูดวัตถุอื่นเข้ามาด้วยแรงโน้มถ่วง เกิดเป็นดาวเคราะห์ในระยะเริ่มต้น แรงโน้มถ่วงที่เพิ่มขึ้นทำให้เกิดการก่อตัวของดาวเคราะห์หินและกลุ่มก๊าซขนาดยักษ์

ดาวเคราะห์ระยะต้นที่อยู่ในย่านที่ปัจจุบันเป็นแถบดาวเคราะห์น้อย ถูกแรงโน้มถ่วงใกล้เคียงก่อกวนจนไม่สามารถรวมตัวกันได้ มันยังคงโคจรรอบดวงอาทิตย์ได้อย่างที่เคยเป็น แต่แยกสลายออกเป็นชิ้นเล็กชิ้นน้อย^[20] วัตถุในย่านนั้นมีความเร็วเฉลี่ยสูงมากเกินไป และการกระจายตัวของดาวเคราะห์ระยะต้นทำให้มันมีแนวโน้มจะแตกออกมากกว่า^[21] และไม่สามารถรวมตัวกันเป็นดาวเคราะห์ที่มีขนาดใหญ่เพียงพอ นอกจากนี้ยังเกิดเหตุการณ์วงโคจรทับซ้อน คือไปซ้อนกับวงโคจรของดาวพฤหัสบดี ทำให้เกิดการรบกวนการเคลื่อนที่ของวัตถุบางชิ้นและดึงพวกมันเข้าไปยังอีกวงโคจรหนึ่ง ย่านอวกาศระหว่างดาวอังคารกับดาวพฤหัสบดีมีวงโคจรทับซ้อนมากมาย บางคราวดาวพฤหัสบดีก็เคลื่อนเข้าใกล้วงโคจรด้านใน เกิดการกระตุ้นเหล่าวัตถุในย่านแถบหลักและทำให้พวกมันเพิ่มความเร็วสัมพัทธ์มากยิ่งขึ้น^[22]

ในยุคเริ่มต้นของระบบสุริยะ ดาวเคราะห์น้อยมีการหลอมละลายไปส่วนหนึ่ง ทำให้องค์ประกอบภายในมีความแตกต่างอย่างมากเมื่อเทียบกับมวล วัตถุยุคดั้งเดิมบางส่วนต้องผ่านกระบวนการเปลี่ยนแปลงอย่างมากในการระเบิดของภูเขาไฟ และทำให้เกิดมหาสมุทร**หินหนืด** อย่างไรก็ตาม เนื่องจากรูปร่างของตัววัตถุเองที่ค่อนข้างเล็ก จึงเกิดช่วงเวลาในการหลอมละลายนี้ค่อนข้างสั้น (เมื่อเทียบกับวัตถุที่ใหญ่กว่ามาก เช่น ดาวเคราะห์) และสิ้นสุดลงในราว 4,500 ล้านปีที่แล้ว ซึ่งนับเป็นเวลาหลายสิบล้านปีแรกๆ ของยุคการก่อตัว^[23] ในเดือนสิงหาคม ค.ศ. 2007 มีการศึกษาผลึกเพทายในอุกกาบาตที่แอนตาร์กติกาที่เชื่อว่ามีกำเนิดจากดาวเคราะห์น้อย **4 เวสตา** ผลการศึกษาชี้ว่ามันถือกำเนิดขึ้นอย่างรวดเร็วภายในช่วงสิบล้านปีแรกของการกำเนิดระบบสุริยะ ซึ่งดาวเคราะห์น้อยอื่นๆ ในแถบหลักก็น่าจะมีกำเนิดในช่วงเดียวกัน^[24]

Problem #1: Tibetan



ལྷོ་བོ་རིག་མཛོད།
རང་དབང་གི་རིག་མཛོད་ཚེན་མོ།

- གཙོ་ངོམ།
- ཁོངས་མི་འདུ་རུ།
- ད་ལྟོ་བའི་བྱ་བ།
- ཉེ་བའི་བོའོ་བཅོམས།
- རང་མོམ་ལོག་ངོམ།
- རོགས་རམས།
- ཞལ་འདེབས།

- ལག་ཆ།
- གང་དག་ལ་སྒྲིལ་པོད།
- འབྲེལ་བའི་བོའོ་བཅོམས།

ཐོ་འགོད། རང་འཇུག།

ཚུམ་ཡིག་ **ལྷོ་བོ་རིག་མཛོད།** ལྷོག་པ། **ཚུམ་སྒྲིག་**

སྲོང་གཙོན་སྒྲིལ་པོའོ་མཛོད་བཅུད་སྒྲིལ།

སྲོང་གཙོན་སྒྲིལ་པོའོ་མཛོད་བཅུད་སྒྲིལ།

[\[ཚུམ་སྒྲིག་\]](#)

ཁོང་གི་ལབ་རྒྱལ་པོའོ་བུ་བཞག་རྒྱུད་འཛིན་གནང་ལྟེ་ མཐའ་བཞིའི་རྒྱལ་སྐོར་སུམ་པ་དང་ཞང་ཞུང་མོགས་མངའ་བོག་ཏུ་བསྐྱུལ་ཏེ་ བོད་གཞིག་འབྲུར་གྱི་རྒྱབ་མཚན་ཏུ་བཞག་ལེགས་འབྲུབ་གནང་བ་ཙམ་མ་ཟད་དམག་དོན་ལམ་ལུགས་གསར་དུ་བརྒྱགས་པ་དང་ ཚབ་སྲིད་ཀྱི་མད་ཐབས་གསར་བ་མང་པོ་ཙམ་ལག་ལེན་བསྐྱར་ དཔལ་འབྱོར་ལམ་ལུགས་མད་ལའང་བསྐྱར་བཅོམ་མང་དུ་གནང་བམ་བོད་མི་རིགས་རང་ཉིད་ཀྱི་ཁུད་ཚོས་ལྷན་པའི་བོའོ་བཅོམ་སྒྲོལ་དཔེར་ན་ འབལ་འཐག་དང་ མཛོམ་རིག་ ལྷར་བཞོམ་ གཤམ་མ་བཞོམ་ གསལ་རྒྱལ་ དདུལ་རྒྱལ་ ལུགས་རྒྱལ་ འོག་ཏུ་བོའོ་བཅོམ་གྱི་ལག་རྒྱལ་གོང་འཕེལ་ཚེ་ཚེར་འབྲོ་ལུབ་པ་བྱུང་ཞིང་། མ་ཟད་མཛོམ་རིག་ལབ་འབག་ལ་འབྲེལ་བ་བརྒྱགས་སྐབས་བོད་ཀྱི་ཚོང་ལམ་གོང་འཕེལ་ལུགས་ཚེན་བཏང་བ་དང་ རིག་གནས་ལའང་ལྷར་བྱུང་མ་ཚོའོང་བའི་འཕེལ་རྒྱུ་ལྷིན་པ་ ཏུ་མ་དེར་པོ་རྒྱལ་དང་ ཚུམ་རིག་ ལྷུག་པ། ལུས་རྒྱལ། ལམ་ལམ་ལག་རྒྱལ། བཞོམ་རིག་ མཛོམ་རིག་ ལྷན་རྒྱལ་ ཚོམ་ལུགས་མོགས་ཉམས་པ་མོར་རྒྱང་དང་མ་ཉམས་གོང་སྒྲིལ་ ལྷར་མེད་གསར་བསྐྱབས་ཀྱི་ཐབས་ལམ་བཞེན་ནས་ལྷོགས་གང་ཅིའི་མད་འཕེལ་རྒྱལ་ལུགས་ཚེན་བྱུང་བར་བཞེན་རིན་མད་གཞལ་དུ་མེད་པའི་བོད་ཀྱི་གནའ་རབས་རིག་གནས་གོང་དུ་སྒྲིལ་བར་ མང་གཞི་སྐྱབས་བཅུན་ཞིག་བཏང་བ་རེད། དེས་མ་ཚང་བལ་བཟའ་དང་རྒྱལ་བཟའ་བོད་དུ་བསྐྱུལ་པ་ནས་བོད་རྒྱ་ དང་བོད་བལ་ མི་རིགས་དབར་མཛོམ་མཐུན་གྱི་འབྲེལ་བ་སྐྱར་བྱུང་མ་ཚོའོང་བ་ཞིག་བཞག་པ་མོགས་གྱི་མཛོམ་བཅུད་ ཉ་ཅང་མང་པམ་བཀའ་རྒྱུན་ལྷན་ཏུ་ཚེའོ།

Problem #1

- Some languages do not separate between words; they either separate between sentences or just when they feel like it
- In others it is highly context sensitive, a “guessing game” to put it in the words of Microsoft (see *Word Breaking Japanese Is Hard* on MSDN Blogs)
- Wikimedia sites in those languages have been left out, for the moment at least

Problem #2: XML

- Wikimedia stopped producing HTML dumps
- Apparently all XPath engines (or at least xsltproc and everything based on LibXML2) load the full XML document in RAM before applying filters
- Good luck extracting <title> and <text> from the 42GB enwiki-latest-pages-articles.xml with that 😊
- Had to write my own XML parser and converter of XML entities (& ' > < ")

Problem #3: wiki syntax

- There is no complete, accurate and up-to-date specification; the best is apparently to just read the 20kLOC parser source
- Most if not all alternative parsers are understandably broken or incomplete
- Ignore everything between [], {} & <> and hope for the best? Still not sufficient 😞
- Curse people who publish incorrect syntax

Problem #4: HTML

- HTML5 has 2125 entities like `é`; for *é*
- People can also directly specify decimal or hexadecimal code points for any Unicode character e.g. using `É`; or `É`; for *é*
- Apparently it is quite common for people to forget parts of URLs so if you are not careful then *server.domain.tld?lotsofcrap&somemore* is split into words and stored in the wordlist

Problem #5: Unicode

- Looking for alphabetic and numeric characters is not sufficient, you have to include non-spacing marks, combining mark and enclosing marks that some languages use for example to merge letters
- Discretionary hyphens (*0xc2ad* or *­* or *­* or *­*) are sometimes used inside words as hints for line breaks; if you make the mistake of treating them like regular hyphens you'll end up breaking those words into pieces

Problem #6: junk


- So are these words or not?
 - Rrrrrrr
 - Llanfairpwllgwyngyllgogerychwyrndrobwlllantysiliogogogoch
 - Taumatawhakatangihangakoauauotamateaturipukakapikimaungahoronukupokaiwhenuakitanatahu
 - Vvttpckeckuoaebdvisackeckuoaebdckeckuoaebdackeckuoaebdyackeckuoaebdvttmzhckeckuoaebdackeckuoaebdyackeckuoaebdpvttneilegelir

Rrrrrrr is the title of a (bad) movie

«Un plaisir presque enfantin et communicatif, dont les effets se font sentir longtemps après.»
Studio

LE PREMIER THRILLER POLICIER PRÉHISTORIQUE !

Il y a 35 000 ans, deux tribus voisines vivaient en paix... à un cheveu près. Pendant que la tribu des Cheveux Propres coulait des jours paisibles en gardant pour elle seule le secret de la formule du shampooing, la tribu des Cheveux Sales se lamentait. Son chef décida d'envoyer un espion pour voler la recette. Mais un événement bien plus grave allait bouleverser la vie des Cheveux Propres : pour la première fois dans l'histoire de l'humanité, un crime venait d'être commis. Comment découvrir son auteur ? Au temps des mammouths et des moutourmes commence la première enquête policière de l'Histoire.



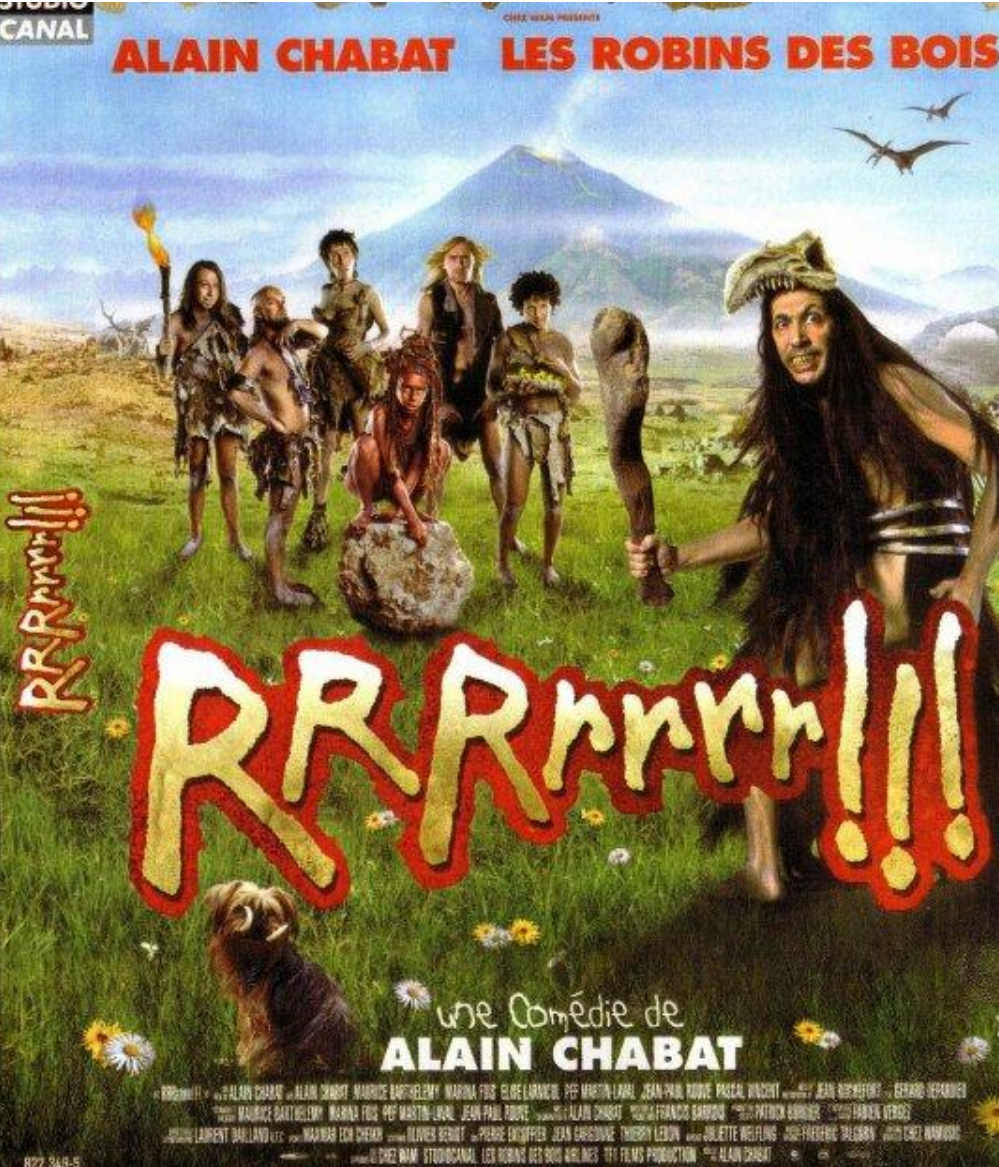
Après «Astérix & Obélix : Mission Cléopâtre», Alain Chabat signe une comédie pré-hystérique qui a fait trembler le box omouth. Catapultez-vous pour un RRRrrrrretour vers le passémouth avec la horde sauvage : les Robins des Bois, Gérard Depardieu et Jean Rochefort !!

DVD 5 langues français 51 sous-titres français
ce film
format 2.35
18/9 temp. 4/3
www.rrrrrrr-lefilm.com

TOUTS PUBLICS
CE DVD EST PROTÉGÉ CONTRE LA COPIE
INTERDIT À LA VENTE

Studio Canal
UNIVERSAL
Aurélien de Lilla
94 rue - Boulevard
CNC
Dolby Digital
DVD
3 475 001 000989
www.studiocanal.com

STUDIO CANAL
ALAIN CHABAT LES ROBINS DES BOIS



RRRrrrr!!!

une Comédie de
ALAIN CHABAT

© 2007 ALAIN CHABAT, ALAIN CHABAT, MAURICE BARTHELEMY, MARINA FOU, ELISE LORANCO, PEP MARTIN-LAVAL, JEAN-PAUL ROUVE, PASCAL VINCENT, JEAN ROCHFERT, GERARD DEPARDIEU, MAURICE BARTHELEMY, MARINA FOU, PEP MARTIN-LAVAL, JEAN-PAUL ROUVE, ALAIN CHABAT, FRANCIS BARRON, PATRICK BORDIER, FABIEN VERGÈS, JUSTIN LAURENT DAILLARD, JEAN-PAUL ROUVE, OLIVIER BEROT, PIERRE ENCOFFRE, JEAN GASCONE, THIERRY LEBON, JULIETTE WELFLING, JOSE-FRÉDÉRIC TALGORN, JACQUES MARQUET, JEAN-PAUL ROUVE, STUDIOCANAL, LES ROBINS DES BOIS AIRLINES, TFI FILMS PRODUCTION, ALAIN CHABAT

822 349-5
DVD DVD
STUDIO CANAL

Llanfair[...] is a city in Wales



Taumata[...] is a hill in New Zealand



LONGEST PLACE NAME IN THE WORLD

Tamatea was a well known chief, warrior and explorer of his time. He is the ancestor of the Ngati Kahungunu people of Porangitua, and acquired many names in consequence to his prowess.

While passing through the inland district of Porangitua, Tamatea encountered the Ngati Raukawa people and had to fight them to get past. In the battle known as 'Whakatu' the latter was killed. Tamatea was so grieved at his loss that he vowed to speak their name at that place and each morning to speak it on the road to give a present to the Kaiaua.

Hence the name indicating the hill on which Tamatea, the chief of great physical culture and prowess, placed a monument in the hill in the memory of his brother.

By Dr. John Campbell, Auckland University
1920-1921, N.Z. A.

Taumatawhakatangihangakoauauotamateaturipukakapikimaungahoronukupokaiwhenuakitanatahu

Problem #6: junk

- Real passwords like *overbuljongterningpakkemesterassistent* (used by one of Per Thorsheim's colleagues 😊) are present less than 200 times in Wikipedia
- Only words present just once have been filtered out, and then again this means ignoring some real words in smaller wikis

Anyway! What do we get?

- wikipedia-wordlist-sraveau-20090325.txt.bz2
 - 213MB
 - 58 427 178 sequences of alphabetic characters
 - Lots and lots of junk
- wikipedia-wordlist-sraveau-20121203.7z
 - 74MB
 - 28 304 682 sequences of **alphanumeric** characters
 - Much, much better quality

Even more fun!



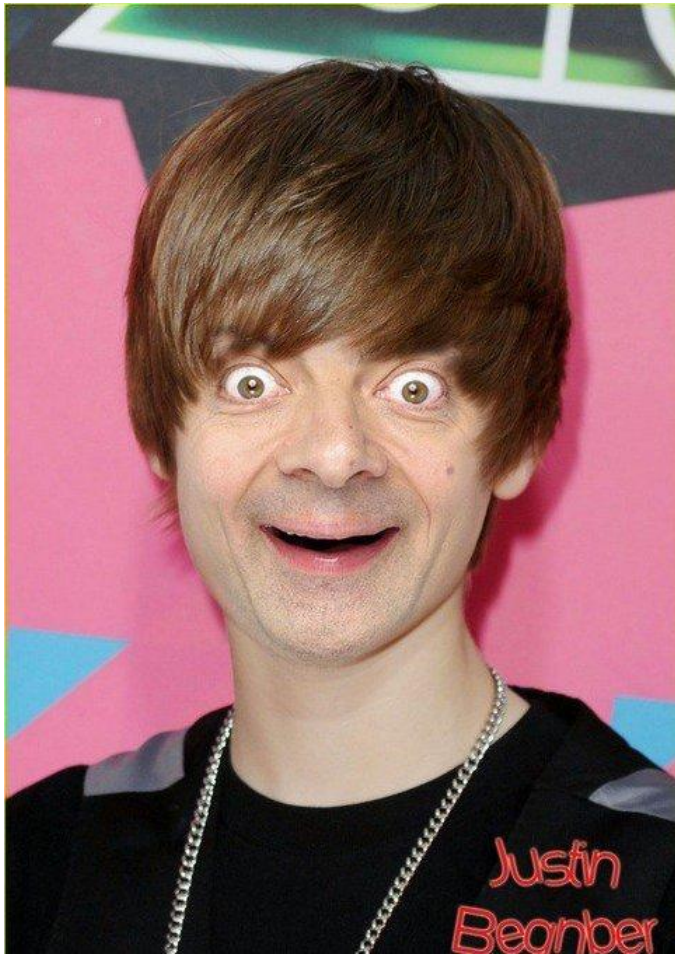
- I am half-French
- I am half-Croatian
- I have a British keyboard
- You can now try to guess my Wi-Fi password more efficiently with

```
extract -wpa  
--keymap gb  
masks/fr.bits  
masks/hr.bits  
wordlist.tree
```


Some measures

Source	Number of words
English Wikimedia sites	3 482 003
German Wikimedia sites	3 536 650
French Wikimedia sites	1 737 776
Norwegian Wikimedia sites	782 606

Even more security!



- With data from November 2012 the wordlist now features all new passwords like *justinbieber*, *iloveyoujustinbieber*, *bieberonomy* and *bieberquake* whatever that means

If you can't wait

- <http://d1.free.fr/ob10I8eGE>
- In the input field below *Recopiez « SomeWord » ci-dessous* retype SomeWord
- Click *Valider et télécharger le fichier*
- MD5 = 423bbb889ea38f0871c21d97a32d7e79
- I'll provide links on Twitter and blog later

But is that really good?

- The wordlist will never be complete
- Secure passwords are leaked just as well
 - Typed in the wrong form field
 - Stored in the shell history
 - Visible in the list of processes
 - Automatically remembered
 - Distributed in an insecure manner

Can you expect people to make sure that every time they enter a password

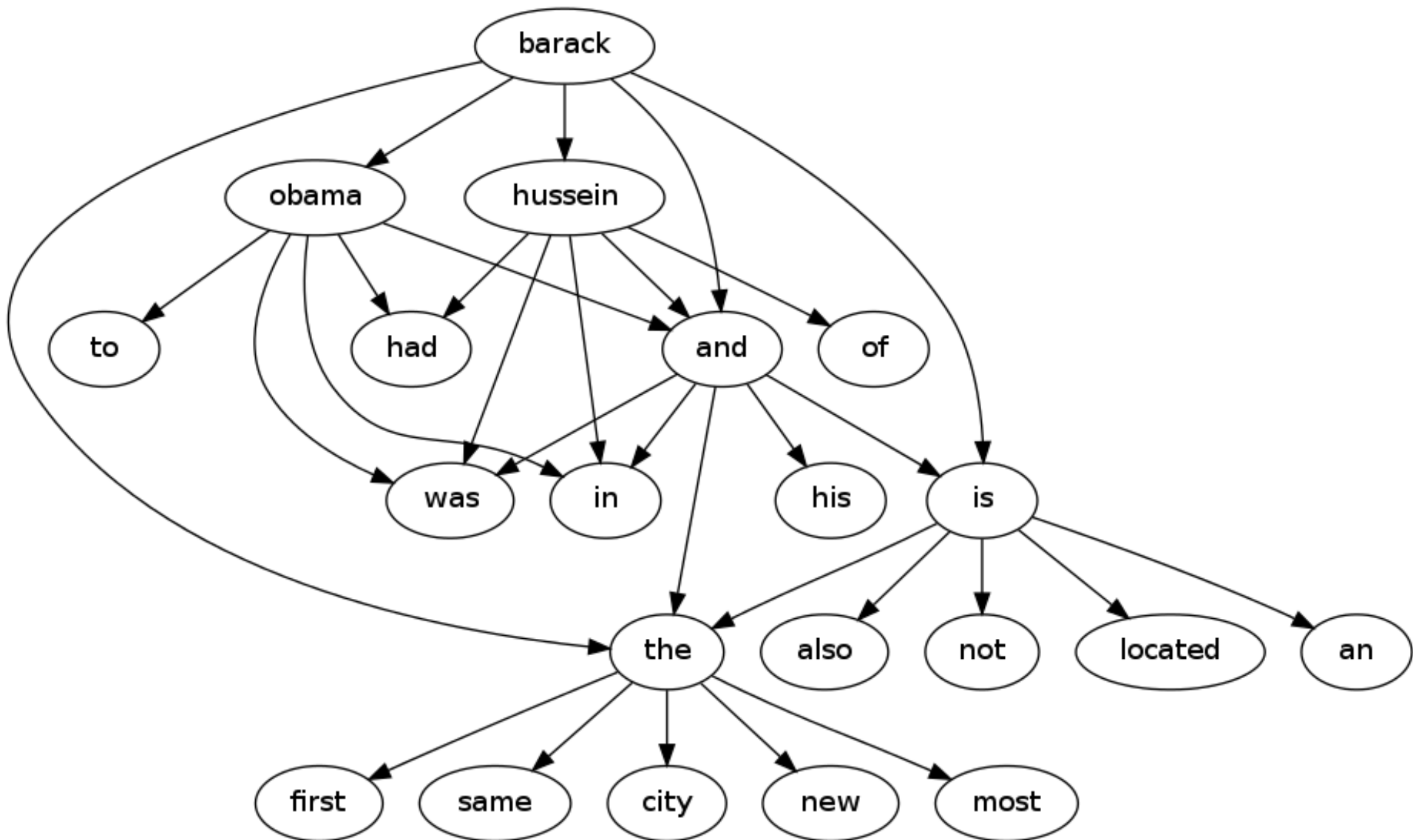
- No person or camera can see
- No microphone, laser or antenna can hear
- No hardware between the keyboard and the computer, inside the keyboard or inside the computer is recording the keystrokes
- No software inside the computer, inside the server or in-between is recording passwords
- Smudges and fingerprints aren't giving it away

Probably not

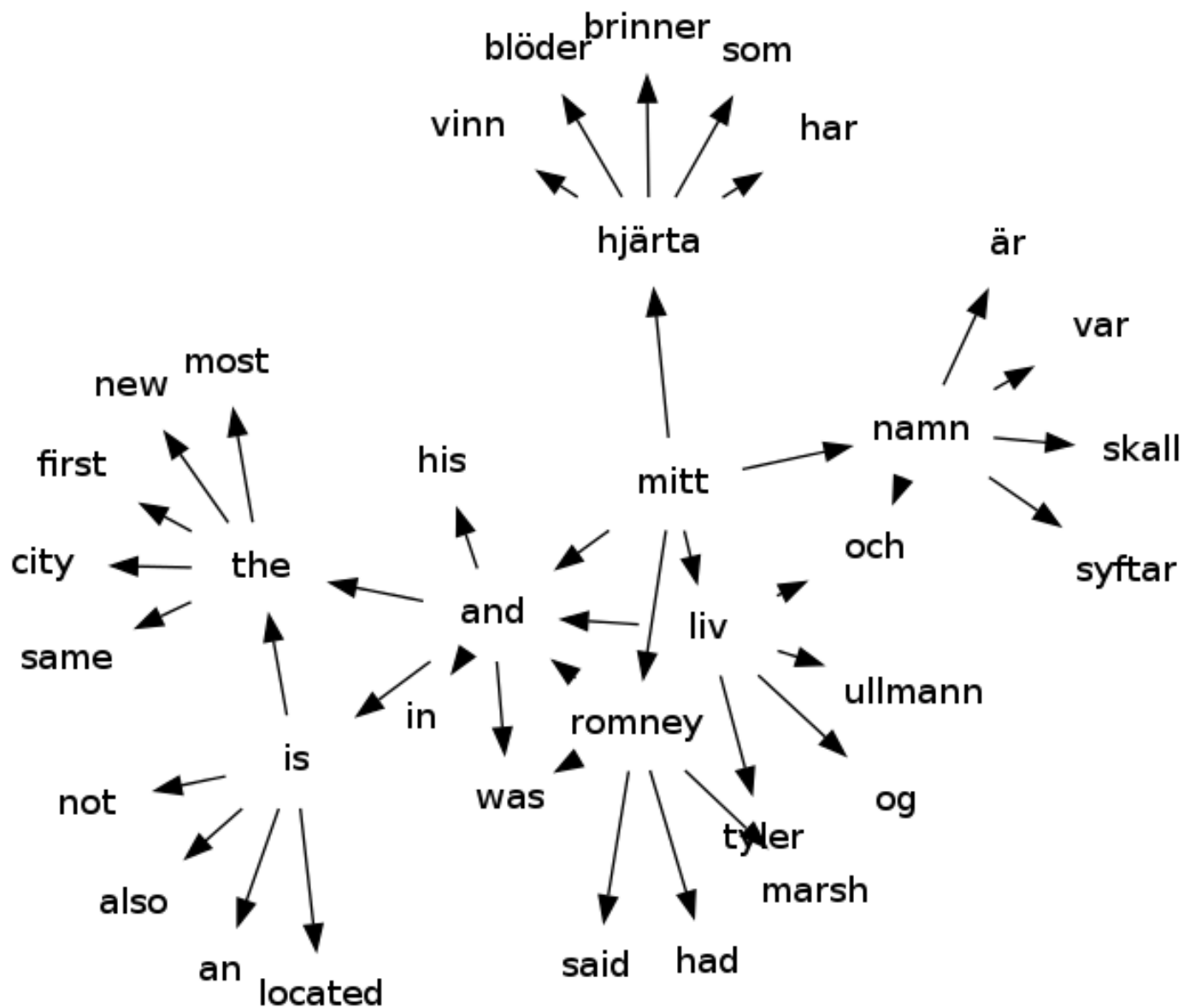
- Ok, maybe you do not have to worry about such “advanced persistent threats”
- But then can we all agree to stop calling password authentication a security feature and instead refer to it as a *convenience* when used alone and as a small *extra* when used in multi-factor authentication?
- Otherwise many people will continue to believe a password prompt makes them perfectly safe

Questions? 😊

Sentences with Wikipedia?



Sentences with Wikipedia?



Alternatives?



Alternatives?



Alternatives?

