Brute Force

Als het goed is hebben we nu een encryptie algoritme. Het algoritme verschuifd de letters x posities. Als je voorbij de Z komt dan begin het weer bij de A. Dus als je de X 5 posities verschuifd dan reulteert dat in een C. Tel maar na.

Dit betekent ook dat als je 26 posities vershuifd je weer terug komt bij dezelfde letter. Of als je 27 cijfers verschuifd is dat hetzelfde als 1 letter vershuiven,

Stel we hebben de volgende tekst:

```
HTP HPPE HLE STPC DELLE RPDNSCPGPY
```

Je weet deze boodschap is gemaakt met het 'verschuif-algoritme'. Je weet alleen de sleutel niet. Hoeveel sleutels zijn er ook alweer? Slecht 25, want bij 26 kom je weer uit op originele boodschap en 27 is hetzelfde als 1.

Dus maak nu een loop waarin je alle sleutels probeert. Decodeer de bovenstaande boodschap door alle mogelijke sleutels te proberen.

> Wat was de originele boodschap?

> Welke sleutel is gebruikt?

Je ziet dat je door alle sleutels te proberen heel snel de orginele boodschap vindt. Dit proberen van alle sleutels heet brute force, brute kracht. Gewoon alles proberen. Bij 25 sleutels lukt dat vrij makkelijk maar als we de sleutels groter maken dan wordt brute force steeds moeilijker.

Symmetrische encryptie

In dit voorbeeld gebruikte we hetzelfde algoritme en eigenlijk ook dezelfde sleutel om een boodschap te encytpen (te versleutelen) en om een boodschap te de-crypten (te ontcijferen). Eigenlijk was het niet helemaal dezelfde sleutel want als we met +1 hadden encrypt dan hadden we -1 of 25 nodig om de decrypten. Maar eigenlijk horen 1 en -1 bij elkaar. Het is immers dezelde sleutel met een ander teken. Als we bij encrypten en decrypten dezelde sleutel gebruiken dan hebben we het over een symmetrische encryptie. Zodra je de sleutel weet dan kan je de code kraken. Dit is anders bij asymmetrische encryptie.

Het voordeel van symmetrische encryptie is dat het lekker snel is om te encrypten en te decrypten. Het nadeel is echter dat als je de sleutel eenmaal weet, dat je dan alle boodschappen kunt ontcijferen.

Asymmetrische encryptie

Bij asymmetrische encryptie is dit anders. Het is werkt wat ingewikkelder en is daardoor wat trager, maar als je de sleutel onderschept, kun je de boodschappen nog niet ontcijferen.

Sleutelgrootte

Omdat we in ons algoritme maar 26 letters hadden, hadden we een keuze uit 1..25 voor de sleutel. Als we hoofd en kleine elttes samen nemen dan zouden we wel wat mer sleutels hebben, maar het schiet nog niet op.

Het schiet wel op als we twee karakters als één teken zien. We gaan dus eignelijk twee karakters omzetten in een nummer. We gebruiken dan geen ASCII tabel meer maar maken onze eigen tabel. AA=0, AB=1, AC=2,.....BA=27, BB= 28, etc. Op deze menier hebben we 676 mogelijke combinaties. Di is 26x26. Als we een groepje van drie karakters nemen dan hebben we al 17576 mogelijke combinaties en dit nummer groeit snel. Als we een groepje van 8 karakters nemen dan hebben we 208 miljard mogelijkehden voor een sleutel, Als we alle sleutels zouden wilen proberen en we kunnen er 1000 per seconden testen dan zouden we ruim in het selchtse geval 6.5 jaar bezig zijn om de sleutel te vinden.

> Vraag: waarom 'in het slechtse geval' zal het 6.5 jaar duren, kan het ook minder lang duren?

Toch is deze methode van letters verschuiven zelfs als we het groepjes doen, niet heel goed.

Ten eerste moet de sleutel heel goed geheim gehouden worden en dat terwijl je hem in eerste instantie wel moet delen. Je zult de sleutel dus een keer moeten opsturen.

Ten tweede kun je met behulp van statistieken voorspellen. Je weet bijvoorbeeld dat de letter e veel vaker voorkomt dan de q. Met die gegevens kun je veel gerichter op zoek gaan naar de sleutel. Zeker als je veel verdleutelde data hebt.

Later gaan we nog eens kijknen naar andere vormen van encryptie. Nu gaan we eerst eens terug nar ons STRIDE model.

Hieronder is een lijst van gebruikersnamen waarmee brute force via SSH op een Linux server is geprobeerd binnen te komen.

```
/var/log/auth.log.1:Dec  5 02:49:52 vps789715 sshd[446357]: Invalid user julia from
45.155.204.39 port 39582
/var/log/auth.log.1:Dec  5 02:49:56 vps789715 sshd[446359]: Invalid user kermit from
45.155.204.39 port 5758
/var/log/auth.log.1:Dec  5 02:50:00 vps789715 sshd[446361]: Invalid user kernel from
45.155.204.39 port 22205
```

```
/var/log/auth.log.1:Dec  5 22:13:50 vps789715 sshd[452901]: Invalid user dietpi from
91.223.67.146 port 7236
/var/log/auth.log.1:Dec  5 22:13:55 vps789715 sshd[452903]: Invalid user pi from 91.223.67.146
port 44171
/var/log/auth.log.1:Dec  5 22:13:59 vps789715 sshd[452905]: Invalid user openhabian from
91.223.67.146 port 24953
/var/log/auth.log.1:Dec  6 02:07:53 vps789715 sshd[453971]: Invalid user admin from
45.155.204.39 port 30624
/var/log/auth.log.1:Dec  6 02:07:56 vps789715 sshd[453973]: Invalid user akiwifi from
45.155.204.39 port 38556
/var/log/auth.log.1:Dec  6 02:07:59 vps789715 sshd[453975]: Invalid user config from
45.155.204.39 port 43557
/var/log/auth.log.1:Dec  6 21:36:39 vps789715 sshd[460616]: Invalid user carlos from
91.223.67.146 port 14752
/var/log/auth.log.1:Dec  6 21:36:42 vps789715 sshd[460618]: Invalid user admin from
91.223.67.146 port 22747
/var/log/auth.log.1:Dec  6 21:36:45 vps789715 sshd[460621]: Invalid user informix from
91.223.67.146 port 28668
/var/log/auth.log.1:Dec  7 01:14:09 vps789715 sshd[462043]: Invalid user admin from
45.155.204.39 port 6832
/var/log/auth.log.1:Dec  7 01:14:12 vps789715 sshd[462045]: Invalid user admin from
45.155.204.39 port 16685
/var/log/auth.log.1:Dec  7 01:14:14 vps789715 sshd[462047]: Invalid user miguel from
45.155.204.39 port 22317
/var/log/auth.log.1:Dec  7 22:24:53 vps789715 sshd[469657]: Invalid user abella from
91.223.67.146 port 41510
/var/log/auth.log.1:Dec  7 22:24:56 vps789715 sshd[469659]: Invalid user antonio from
91.223.67.146 port 30818
/var/log/auth.log.1:Dec  8 01:39:51 vps789715 sshd[470718]: Invalid user admin from
45.155.204.39 port 53722
/var/log/auth.log.1:Dec  8 01:39:54 vps789715 sshd[470720]: Invalid user xml from
45.155.204.39 port 16602
/var/log/auth.log.1:Dec  8 01:39:58 vps789715 sshd[470722]: Invalid user gns3 from
45.155.204.39 port 36374
/var/log/auth.log.1:Dec  8 22:38:56 vps789715 sshd[480723]: Invalid user linktechs from
91.223.67.146 port 39741
/var/log/auth.log.1:Dec  8 22:38:59 vps789715 sshd[480725]: Invalid user localadmin from
91.223.67.146 port 59244
/var/log/auth.log.1:Dec  8 22:39:02 vps789715 sshd[480792]: Invalid user login from
91.223.67.146 port 28668
```

```
/var/log/auth.log.1:Dec  8 22:39:05 vps789715 sshd[480794]: Invalid user login from
91.223.67.146 port 37396
/var/log/auth.log.1:Dec  8 22:39:09 vps789715 sshd[480796]: Invalid user mac from
91.223.67.146 port 39889
/var/log/auth.log.1:Dec  9 06:40:56 vps789715 sshd[493250]: Invalid user netgear from
45.155.204.39 port 30211
/var/log/auth.log.1:Dec  9 06:40:59 vps789715 sshd[493252]: Invalid user admin from
45.155.204.39 port 33234
/var/log/auth.log.1:Dec  9 06:41:06 vps789715 sshd[493256]: Invalid user lena from
45.155.204.39 port 39205
/var/log/auth.log.1:Dec  9 06:41:10 vps789715 sshd[493258]: Invalid user linaro from
45.155.204.39 port 41967
/var/log/auth.log.1:Dec  9 23:02:03 vps789715 sshd[506238]: Invalid user mira from
91.223.67.146 port 14146
/var/log/auth.log.1:Dec  9 23:02:07 vps789715 sshd[506240]: Invalid user mother from
91.223.67.146 port 42884
/var/log/auth.log.1:Dec  9 23:02:10 vps789715 sshd[506242]: Invalid user music from
91.223.67.146 port 10022
/var/log/auth.log.1:Dec  9 23:02:17 vps789715 sshd[506246]: Invalid user natalia from
91.223.67.146 port 38994
/var/log/auth.log.1:Dec 10 06:44:23 vps789715 sshd[508843]: Invalid user mailto from
45.155.204.39 port 22873
/var/log/auth.log.1:Dec 10 06:44:27 vps789715 sshd[508845]: Invalid user manager from
45.155.204.39 port 25270
/var/log/auth.log.1:Dec 10 06:44:29 vps789715 sshd[508847]: Invalid user media from
45.155.204.39 port 26638
/var/log/auth.log.1:Dec 10 06:44:34 vps789715 sshd[508849]: Invalid user michael from
45.155.204.39 port 29436
/var/log/auth.log.1:Dec 10 06:44:36 vps789715 sshd[508851]: Invalid user michelle from
45.155.204.39 port 30938
/var/log/auth.log.1:Dec 10 23:17:07 vps789715 sshd[515371]: Invalid user optiproerp from
91.223.67.146 port 20045
/var/log/auth.log.1:Dec 10 23:17:11 vps789715 sshd[515373]: Invalid user pablo from
91.223.67.146 port 21729
/var/log/auth.log.1:Dec 10 23:17:14 vps789715 sshd[515375]: Invalid user patrol from
91.223.67.146 port 15725
/var/log/auth.log.1:Dec 10 23:17:18 vps789715 sshd[515377]: Invalid user pc1 from
91.223.67.146 port 1109
/var/log/auth.log.1:Dec 10 23:17:23 vps789715 sshd[515379]: Invalid user pedro from
91.223.67.146 port 42140
```

```
/var/log/auth.log.1:Dec 11 06:37:48 vps789715 sshd[518052]: Invalid user nelson from
45.155.204.39 port 15185
/var/log/auth.log.1:Dec 11 06:37:50 vps789715 sshd[518054]: Invalid user netgear from
45.155.204.39 port 17289
/var/log/auth.log.1:Dec 11 06:37:54 vps789715 sshd[518056]: Invalid user nico from
45.155.204.39 port 21331
/var/log/auth.log.1:Dec 11 06:37:57 vps789715 sshd[518058]: Invalid user nsa from
45.155.204.39 port 25242
/var/log/auth.log.1:Dec 11 06:38:00 vps789715 sshd[518060]: Invalid user operator from
45.155.204.39 port 29352
/var/log/auth.log.1:Dec 11 16:44:43 vps789715 sshd[521894]: Invalid user u2078299 from
62.194.183.33 port 54137
/var/log/auth.log.1:Dec 11 16:47:07 vps789715 sshd[521898]: Invalid user u2078299 from
62.194.183.33 port 54143
```

Revision #5
Created 2019-09-17 16:39:27 UTC by Admin
Updated 2021-12-14 20:12:21 UTC by Max