IT & Security

Aspecten van security

- Confidentiality : gegevens die vertrouwelijk zijn moeten vertrouwelijk blijven. Dat geldt bij versturen (onderweg mag niemand het kunnen lezen), maar ook bij opslaan (onbevoegden moeten er niet bij kunnen komen)

- Integrity : gegevens mogen niet ongewild, en zonder dat men het doorheeft, veranderd worden.

- Availability : gegevens / diensten mogen niet ongewild onbeschikbaar worden (door bijv. een aanval)

Encryptie

- Veel verschillende soorten encryptie:

- Symmetrisch, o.a.
  - Ceasar, Vigenère (oud)
  - DES
  - AES

- Asymmetrisch:
  - Diffie-Hellman
  - RSA
  - ElGamal

Ontcijfer de volgende zin

xfmlpn jfefsffm!

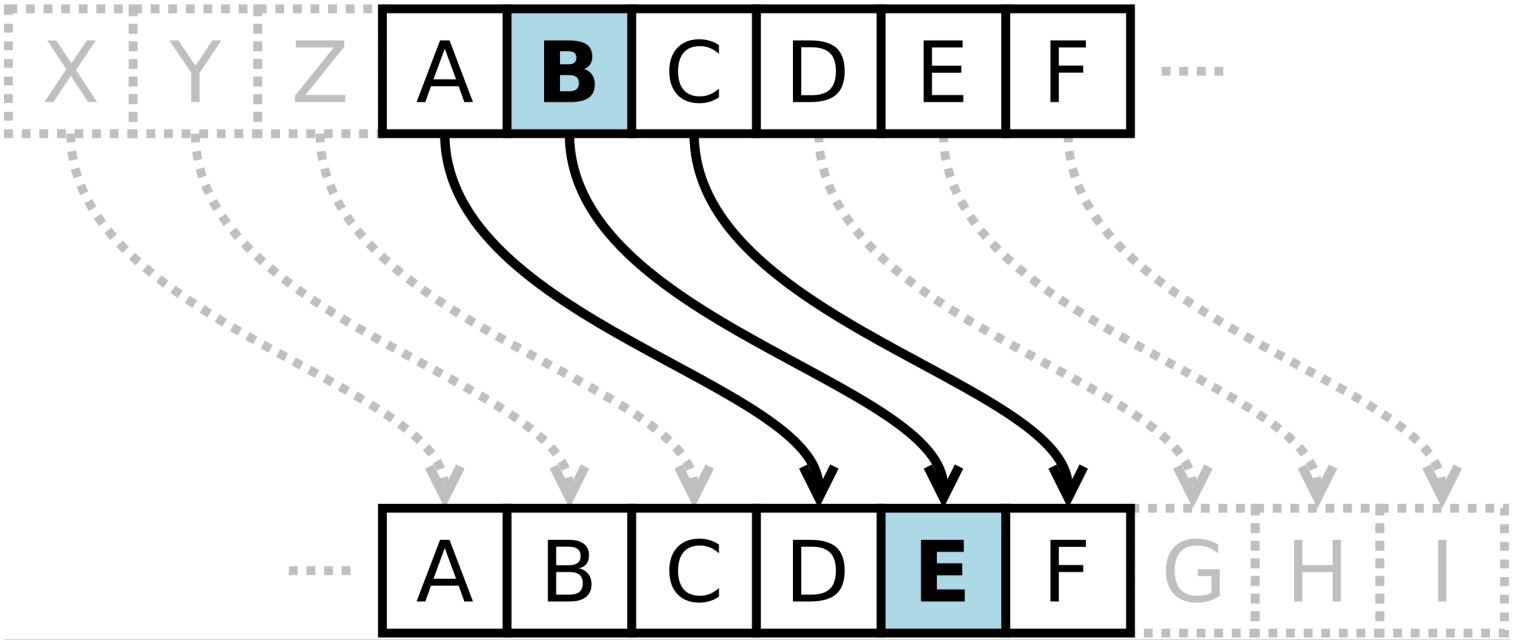
Substitutiecijfers

Het vervangen van een of meerdere letters (of bits / bytes)

Hoe te kraken?

Ceasar-encryptie

- Verschuift simpelweg de letters.
- Sleutel is het ceasarcijfer: hoeveel letters moet je doorschuiven



Vigenere-encryptie

- Als caesar, maar dan met meerdere verschuivingen / alfabetten
- Sleutel is een codewoord waarbij iedere letter de alfabet-rotatie aangeeft (vanaf de a bezien). Sleutel wordt zo vaak als nodig achter elkaar geplakt.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Substitutiecijfers

Ceasarsubstitutie: monoalfabetisch
Vigenère: polyalfabetisch

Transpositiecijfers

Het anders rangschikken van een of meerdere letters (of bits / bytes)

One time pad

Versleutelen met een niet herhalende, echte random sleutel.
In principe onkraakbaar.
Hergebruik van sleutel verboden

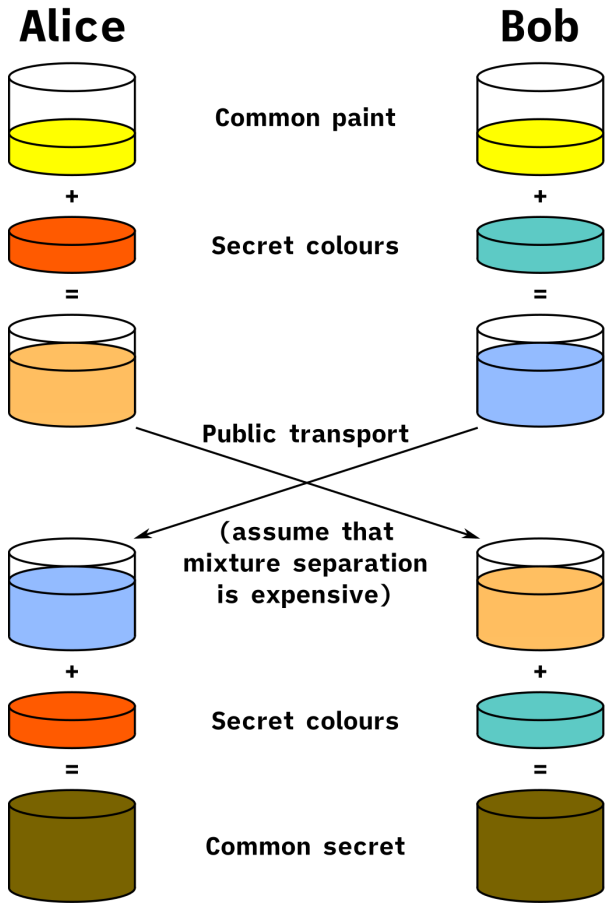
Asymmetrische encryptie

- Verzender en ontvanger hebben niet dezelfde gegevens.
- Een deel van de sleutel blijft privé
- Werkt met modulus en priemgetallen

- Youtube:
  - Intro
  - Achtergrond en mogelijkheden
  - Extra uitleg
  - De wiskundige kant

Diffie-Hellman

- Probleem: twee partijen willen graag via met behulp van symmetrische encryptie (zoals AES) beveiligen, maar hoe zorgen we ervoor dat we het eens worden over de sleutel zonder dat we die open en bloot versturen?
- Oplossing: sleuteluitwisselingsalgoritme van Diffie-Hellman

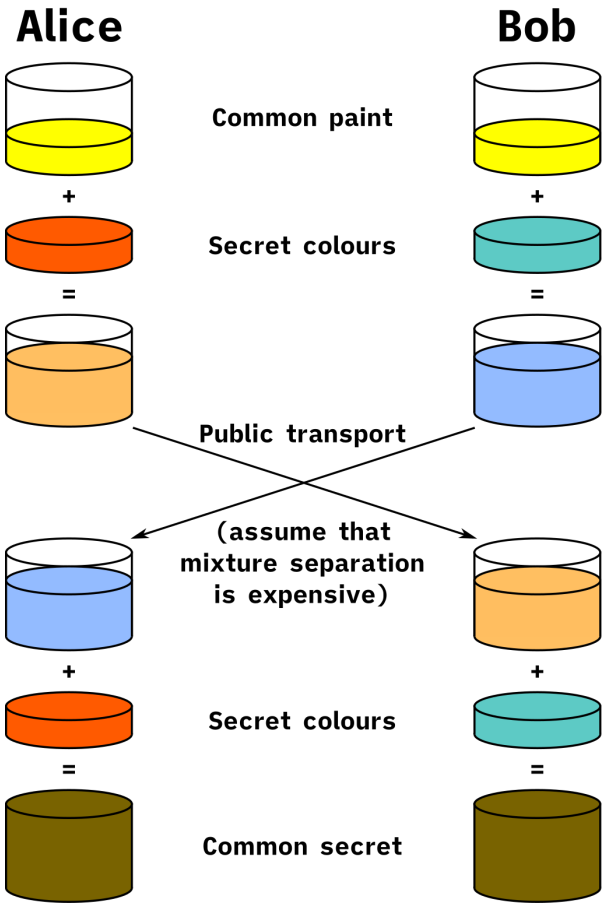


Diffie-Hellman

- Alice en Bob spreken af: priemgetal *p* en een ‘grondgetal’ *g* en communiceren dit met elkaar

- Alice en Bob kiezen allebei een random heel getal
  a voor Alice
  b voor Bob
  Alice rekent uit en stuur naar Bob: $g^a \bmod p$ (de uitkomst heet *A*)
  Bob rekent uit en stuurt naar Alice: $g^b \bmod p$ (de uitkomst heet *B*)

- Alice rekent uit: $B^a \bmod p$
  Bob rekent uit $A^b \bmod p$
  De uitkomst is voor Alice en Bob gelijk.
  Deze uitkomst is dan de sleutel waarmee ze de rest van de communicatie gaan versleutelen



Diffie-Hellman

- Alice en Bob spreken af: priemgetal p en een ‘grondgetal’ g en communiceren dit met elkaar
- p = 23
  g = 5

- Alice en Bob kiezen allebei een random heel getal
  a voor Alice
  b voor Bob
  Alice rekent uit en stuur naar Bob: $g^a \bmod p$ (de uitkomst heet A)
  Bob rekent uit en stuurt naar Alice: $g^b \bmod p$ (de uitkomst heet B)
- Alice kiest a = 4
  en verstuurt A: $5^4 \bmod 23 = 4$
  Bob kiest b = 3
  en verstuurt B: $5^3 \bmod 23 = 10$

- Alice rekent uit: $B^a \bmod p$
  Bob rekent uit $A^b \bmod p$
  De uitkomst is voor Alice en Bob gelijk.
  Deze uitkomst is dan de sleutel waarmee ze de rest van de communicatie gaan versleutelen
- Alice rekent uit: $B^a \bmod p$
  $10^4 \bmod 23 = 18$
  Bob rekent uit $A^b \bmod p$
  $4^3 \bmod 23 = 18$

  De sleutel is dus 18

Diffie-Hellman

- Alice en Bob spreken af: priemgetal p en een ‘grondgetal’ g en communiceren dit met elkaar
- Alice en Bob kiezen allebei een random heel getal
  a voor Alice
  b voor Bob
  Alice rekent uit en stuur naar Bob: $g^a \bmod p$ (de uitkomst heet A)
  Bob rekent uit en stuurt naar Alice: $g^b \bmod p$ (de uitkomst heet B)
- Alice rekent uit: $B^a \bmod p$
  Bob rekent uit $A^b \bmod p$
  De uitkomst is voor Alice en Bob gelijk.
  Deze uitkomst is dan de sleutel waarmee ze de rest van de communicatie gaan versleutelen

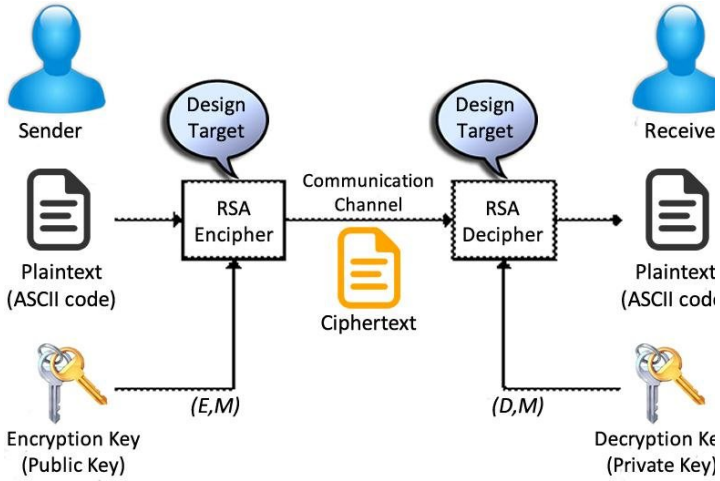
- Eve (de luistervink) kent p en g
- Eve kent WEL A en B
  Eve kent NIET a en b
- Omdat Eve nooit a en b heeft kunnen opvangen (want die houden Alice en Bob geheim), heeft ze nooit genoeg informatie om de sleutel uit te rekenen.

Diffie-Hellman

- Op de toets krijg je sowieso p en g

RSA

- Asymmetrisch
- Ontworpen door Ron Rivest, Adi Shamir en Len Adleman in jaren 1977 (GCHQ in 1973 maar was topgeheim)
- Onder andere gebruikt in SSL-certificaten



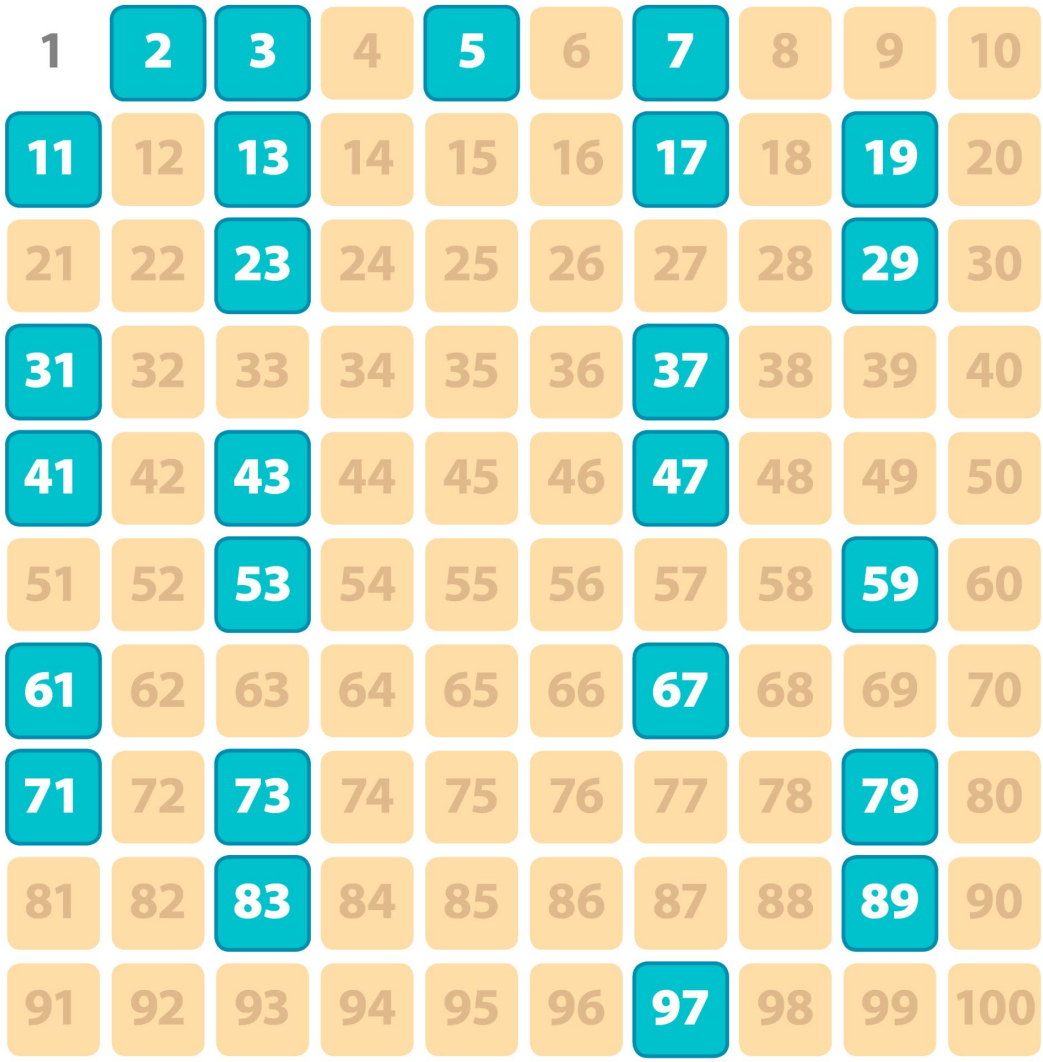
RSA - hoe werkt het?

- Priemgetallen
- Ontbinden in factoren
- Grootste gemene deler
- Modulo rekenen

Priemgetallen

- Een priemgetal is een natuurlijk getal groter dan 1 dat slechts twee natuurlijke getallen als deler heeft, namelijk 1 en zichzelf.
- Kleinste priemgetal is …
- Welke getallen kleiner dan 50 zijn een priemgetal?

Priemgetallen < 100



Ontbinden in factoren

- Elk natuurlijk getal dat geen priemgetal is, kun je schrijven als vermenigvuldiging van priemgetallen
- Bijvoorbeeld:
  - 8 -> 2 x 2 x 2
  - 18 -> 2 x 9 -> 2 x 3 x 3
  - 99 -> 3 x 33 -> 3 x 3 x 11
  - 100 -> 2 x 50 -> 2 x 2 x 25 -> 2 x 2 x 5 x 5

Ontbind in factoren:

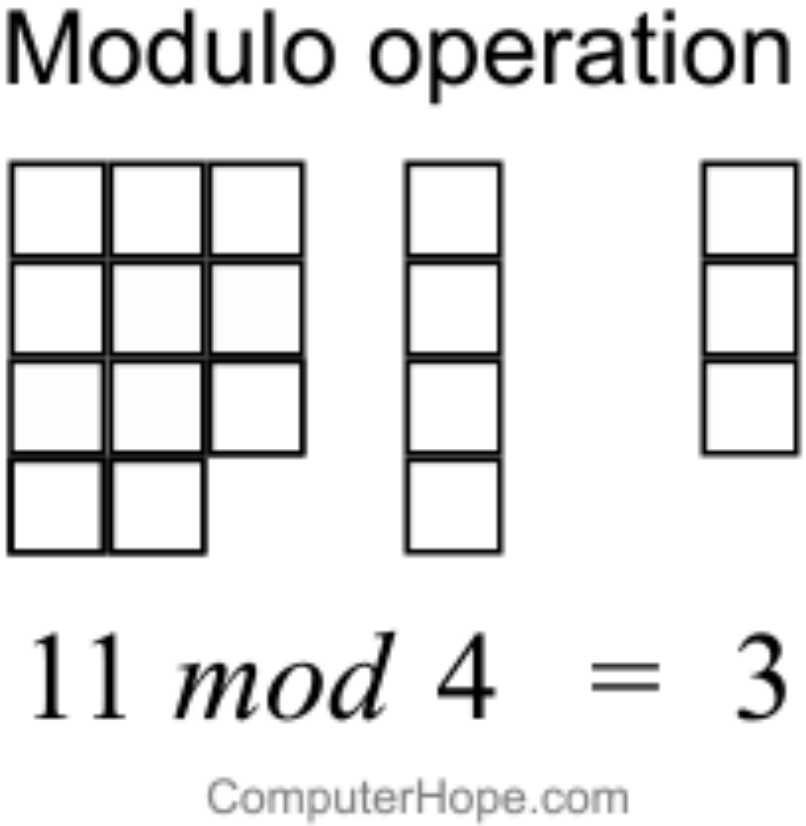
- 42
- 43
- 74
- 162

Ontbind in factoren:

- 42: 2 x 3 x 7
- 43: instinker, is priemgetal
- 74: 2 x 37
- 162: 2 x 3 x 3 x 3 x 3

Modulo rekenen

- Ook wel klok-rekenen of delen met rest met hele getallen genoemd
- 16:15 uur -> 4:15 uur. Je haalt er 12 af
- 32:15 uur (als dat zou bestaan) -> 8:15 uur. Want 12 past twee keer in 32 en dan hou je 32-24 = 8 over
- Dus 32 mod 12 = 8
- Of netter: 32 ≡ 8 (mod 12)



32 en 8 zijn congruent modulo 12

RSA in 5 stappen

- Kies willekeurig twee priemgetallen p en q

RSA in 5 stappen

- Kies willekeurig twee priemgetallen p en q
  p = 3, q = 47

RSA in 5 stappen

- Kies willekeurig twee priemgetallen p en q
  p = 3, q = 47

- Bereken n = p x q.

RSA in 5 stappen

- Kies willekeurig twee priemgetallen p en q
  p = 3, q = 47

- Bereken n = p x q. 141

RSA in 5 stappen

- Kies willekeurig twee priemgetallen p en q
  p = 3, q = 47

- Bereken n = p x q. n = 141

RSA in 5 stappen

- Kies willekeurig twee priemgetallen p en q
  p = 3, q = 47
- Bereken n = p x q. n = 141
- Bereken K.

Getal K

- K is “het aantal getallen kleiner dan n dat géén priemfactor met n gemeenschappelijk heeft”

- n is 141, bestaat uit priemfactoren … (bedenk zelf)

Getal K

- K is “het aantal getallen kleiner dan n dat géén priemfactor met n gemeenschappelijk heeft”

- n is 141, bestaat uit priemfactoren 3 x 47

- Welke getallen getallen van 2 t/m 140 hebben niet de priemfactoren 3 en / of 47?
  3, 6, 9, 12, 15, 18, 21, etc. (tafel van 3)
  47, 94 (eerste twee uit de tafel van 47)

Dat kan gemakkelijker!

Hier volgt een trucje:

Getal K

- K is “het aantal getallen kleiner dan n dat géén priemfactor met n gemeenschappelijk heeft”

- K = (p-1) x (q-1)

Getal K

- K is “het aantal getallen kleiner dan n dat géén priemfactor met n gemeenschappelijk heeft”

- K = (p-1) x (q-1)

- K = (3-1) x (47-1)
  K = 2 x 46
  K = 92

RSA in 5 stappen

- Kies willekeurig twee priemgetallen p en q
  p = 3, q = 47
- Bereken n = p x q. n = 141
- Bereken K. K = 92
- Bereken getal d.

d

- “getal < K dat 1 als grootste gemeenschappelijke deler met K heeft.”
- M.a.w: ontbonden in factoren moeten K en d uit totaal andere factoren bestaan
- K = 92 = 2 x 2 x 23
- d mag dus zijn 3, 5, 7, 9, 11, 13, 15, ..
- We kiezen nu voor 7

RSA in 5 stappen

- Kies willekeurig twee priemgetallen p en q
  p = 3, q = 47
- Bereken n = p x q. n = 141
- Bereken K. K = 92
- Bereken getal d. d = 7

RSA in 5 stappen

- Kies willekeurig twee priemgetallen p en q
  p = 3, q = 47
- Bereken n = p x q. n = 141
- Bereken K. K = 92
- Bereken getal d. d = 7
- Bereken getal e.

e

- Kies e zo dat (d x e) mod K = 1
- dus: (7 x e) mod 92 = 1
- Welke getallen zijn 1 onder mod 92?
  Ieder product van 92, plus 1.
  Zoek er een deelbaar door d (in dit geval 7)
  93, 185, 277, 369, 461, 553, …
- Soms snel te vinden, soms niet.
- e = 553 / 7 = 79

RSA in 5 stappen

- Kies willekeurig twee priemgetallen p en q
  p = 3, q = 47
- Bereken n = p x q. n = 141
- Bereken K. Dit wordt de modulus. K = 92
- Bereken getal d. d = 7
- Bereken getal e. e = 79
- Publieke sleutel is (d, n), privésleutel is (e, n)

RSA in 5 stappen

- p = 3, q = 47, n = 141, K = 92, d = 7, e = 79
- Versleutelen met de publieke sleutel gaat door machtsverheffen:
  cijfertekstgetal = klaretekstgetal ^{e} (mod n)
- Ontcijferen is met de andere sleutel:
  klaretekstgetal = cijfertekstgetal^{d} (mod n)

RSA in 5 stappen

- p = 3, q = 47, n = 141, K = 92, d = 7, e = 79
- Versleutelen met de publieke sleutel gaat door machtsverheffen:
  cijfertekstgetal = klaretekstgetal ^{e} (mod n)
- Ontcijferen is met de andere sleutel:
  klaretekstgetal = cijfertekstgetal^{d} (mod n)

- Stel ik wil het getal **65** versturen:
  65^{79} (mod 141)

RSA in 5 stappen

$65^{79} \pmod{141} = ((65^4)^{18} \times 65^4 \times 65^3) \pmod{141}$

$= (65^4 \pmod{141})^{18} \pmod{141} \times 65^4 \pmod{141} \times 65^3 \pmod{141}$

$= 25^{18} \pmod{141} \times 65^4 \pmod{141} \times 65^3 \pmod{141}$

$= 25^{18} \pmod{141} \times 25 \times 98$

$= (25^3 \pmod{141})^6 \pmod{141} \times 25 \times 98$

$= (15625 \pmod{141})^6 \pmod{141} \times 25 \times 98$

$= 115^6 \pmod{141} \times 25 \times 98$

$= 4 \times 25 \times 98 \pmod{141}$

$= 9800 \bmod 141 = \mathbf{71}$

RSA in 5 stappen

- p = 3, q = 47, n = 141, K = 92, d = 7, e = 79
- Versleutelen met de publieke sleutel gaat door machtsverheffen:
  cijfertekstgetal = klaretekstgetal ^{e} *(mod n)*
- 65 is versleuteld 71, dat wordt verstuurd

RSA in 5 stappen

- p = 3, q = 47, n = 141, K = 92, d = 7, e = 79
- Versleutelen met de publieke sleutel gaat door machtsverheffen:
  cijfertekstgetal = klaretekstgetal ^{e} (mod n)
- 65^{79} (mod 141) = 71 —> versleuteld
- Ontcijferen is met de andere sleutel:
  klaretekstgetal = cijfertekstgetal^{d} (mod n)

- Ontvanger ziet het getal 71. Om dit te ontsleutelen bereken je: *71^{7} (mod 141)*

RSA in 5 stappen

- $71^7 \pmod{141}$

$= (71^3 \pmod{141} \times 71^4 \pmod{141})$

$= 357911 \pmod{141} \times 25411681 \pmod{141}$

$= (53 \times 97) \pmod{141}$

$= 5141 \bmod 141 = 65$

Gebruik van GR

- Modulus bij RSA: gebruik de functie MOD_EXP
  (optn F6 F4 F6 F5)

- Vinden van e: gebruik tabellen (onder 'menu' 7):
  X: 1 t/m 40 (domein in te vullen onder SET)
  Y1: K*X + 1 (K weet je en vul je in)
  Y2: Y1 / d (d weet je en vul je in)

  een heel getal in kolom Y2 is een geldige waarde voor e

Hash

- Een hashfunctie neemt een input van willekeurige lengte en geeft een output van een vast aantal tekens (of eigenlijk bits), ongeacht de lengte van de input

- Dit is een ‘one way function’: de ene kant op heel gemakkelijk, de andere kant op heel erg moeilijk. Uit een hash de input berekenen is bij goede hashfuncties praktisch onmogelijk.

- Probeer eens op https://passwordsgenerator.net/sha256-hash-generator/

Gebruik van hashing

- Je kunt controleren of data is veranderd / hetzelfde is: andere data (zelfs al 1 letter) geeft een andere hashwaarde. Bijvoorbeeld om te controleren of een bestand dat je download niet stiekem door hackers is besmet.

- Een webwinkel slaat als het goed is wachtwoorden op als hash. Zo zijn de wachtwoorden zelf nooit te achterhalen maar kun je wel controleren of men het juiste wachtwoord geeft. Dat moet namelijk dezelfde hash opleveren.

Gebruik van hashing

- Je kunt met behulp van hashing dus gemakkelijk herkennen of twee stukken digitale informatie hetzelfde zijn.

- Een hash werkt zo dus als een digitale vingerafdruk. Daarmee kun je:

  - Controleren of men het goede wachtwoord heeft ingevuld zonder het wachtwoord zelf ergens op te slaan.

  - Het als controle gebruiken om te voorkomen dat een bestand veranderd wordt. De authenticiteit van de hash moet dan wel gegarandeerd zijn.

  - Het gebruiken om snel identieke bestanden op te sporen.

Collision

- Een hashfunctie geeft altijd een output van een vaste lengte. Het aantal mogelijke uitkomsten is hierdoor begrensd. Het aantal mogelijke inputs is echter onbeperkt. Er zullen daardoor meerdere verschillende inputs zijn die dezelfde hashwaarde als output hebben. Dit heet collision.

- Bij een goed hash-algoritme is de kans dat dit in praktijk voorkomt vrijwel 0.

Salting

- Om het extra moeilijk te maken om een hash met een woordenboekaanval te herleiden naar de oorspronkelijke input, kun je ervoor kiezen vóór het uitvoeren van de hash de input te voorzien van extra bits / bytes / tekens. Dit heet salting.

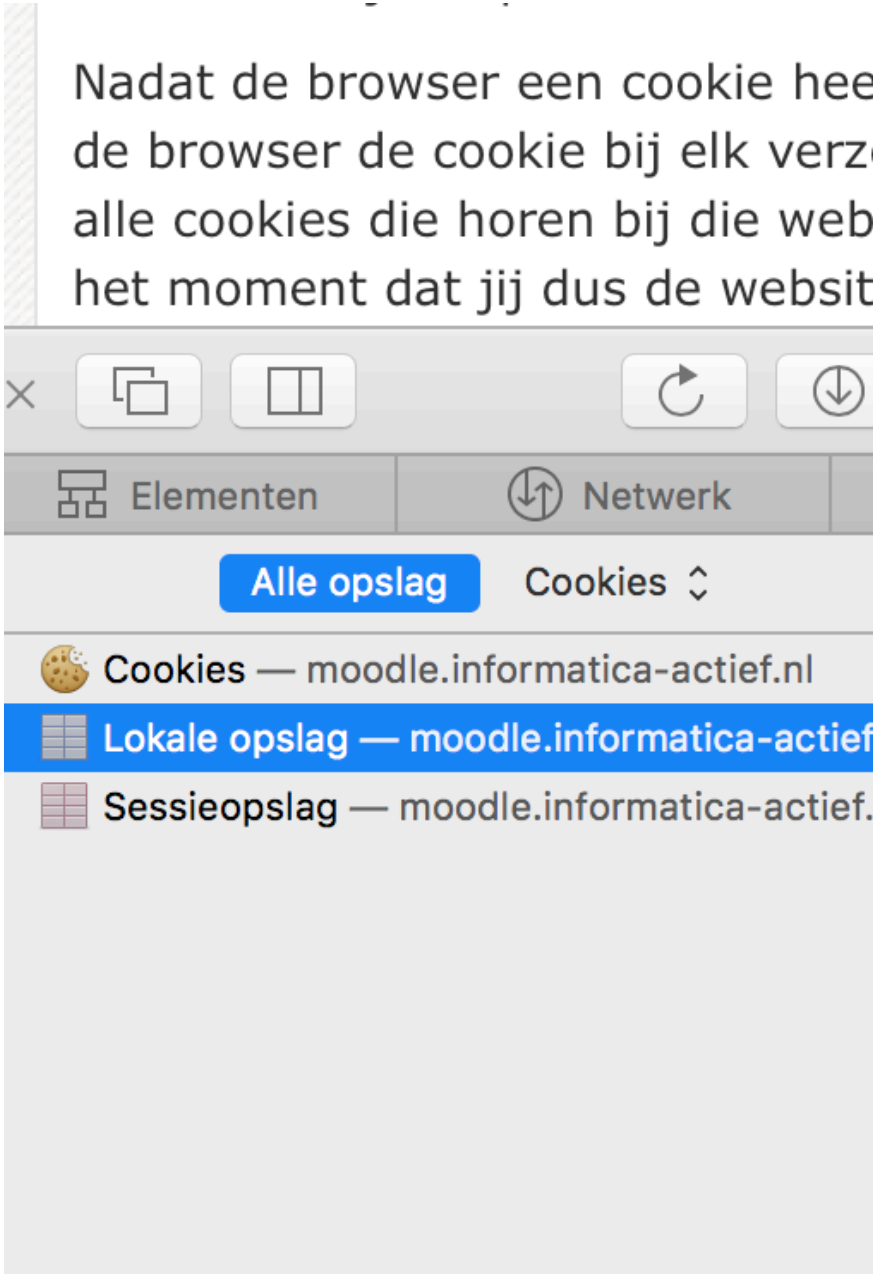
- Voorwaarde is natuurlijk dat je dit altijd op dezelfde manier doet.

Cookies

- Een webbrowser houdt geen contact met de server waar de website op staat
- Ieder verzoek staat volkomen los van het vorige.
- Probleem bij boodschappenmandje van webwinkel

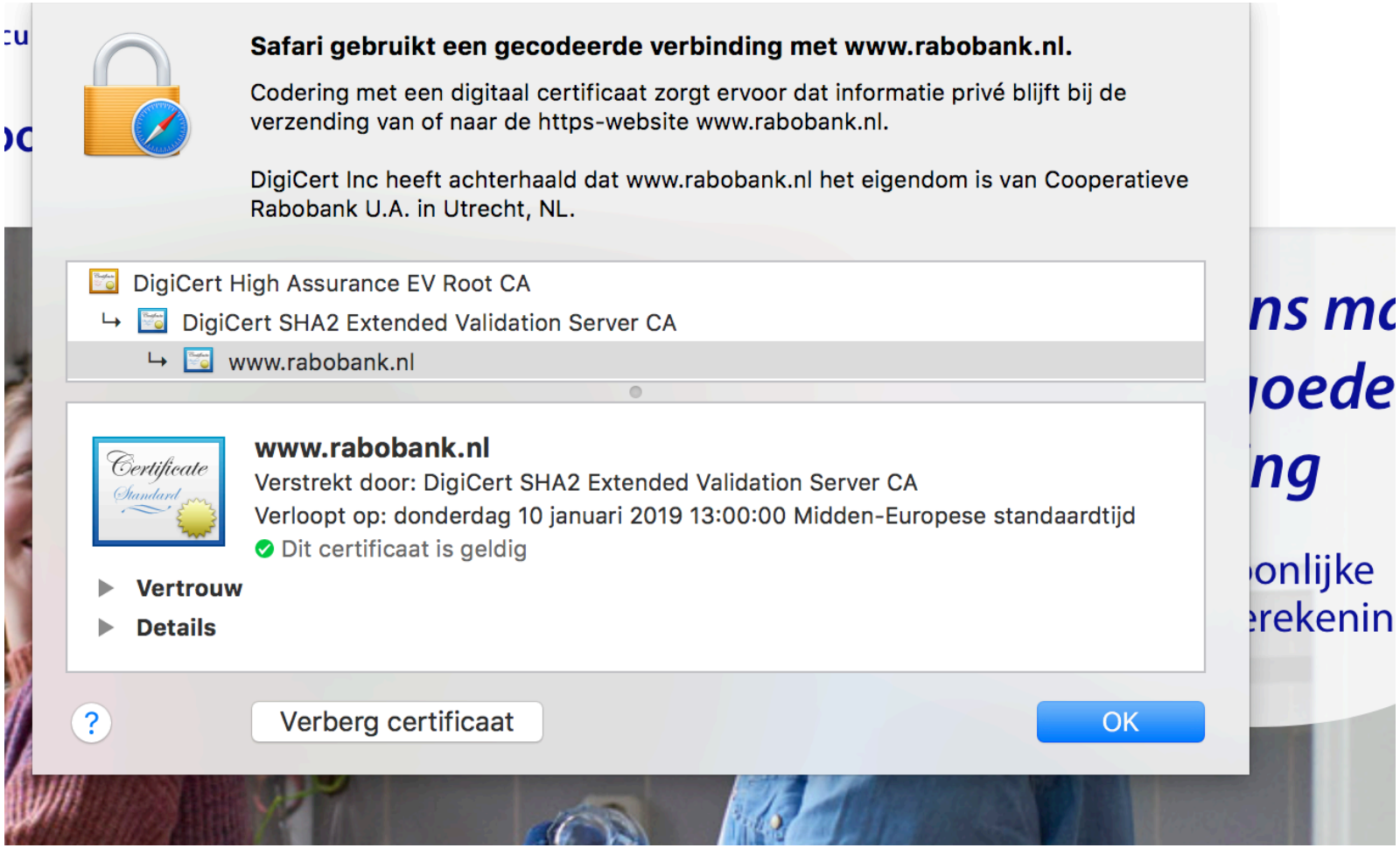
Hoe werken cookies?

Cookies inspecteren



Privacy

- Wat hebben cookies met privacy te maken?
- Surfgedrag bijhouden
- Niet alleen eigenaar van websites, maar ook third parties



webcertificaten

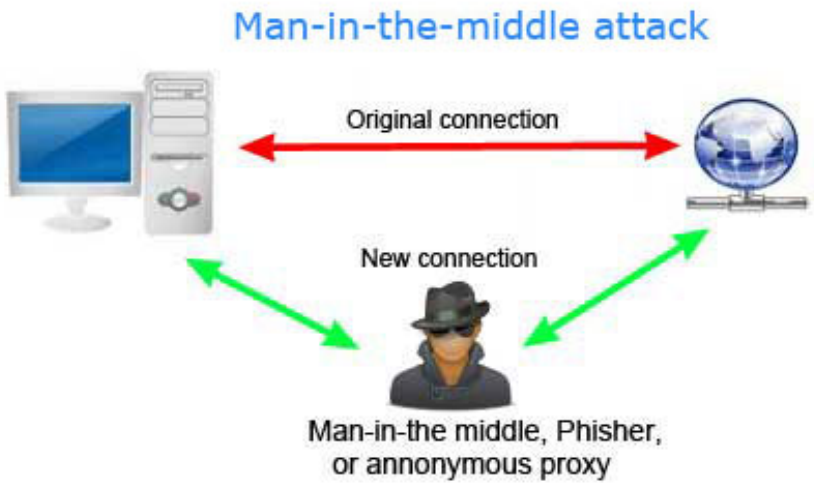
§

Functie

- Authenticatie
- Versleuteling

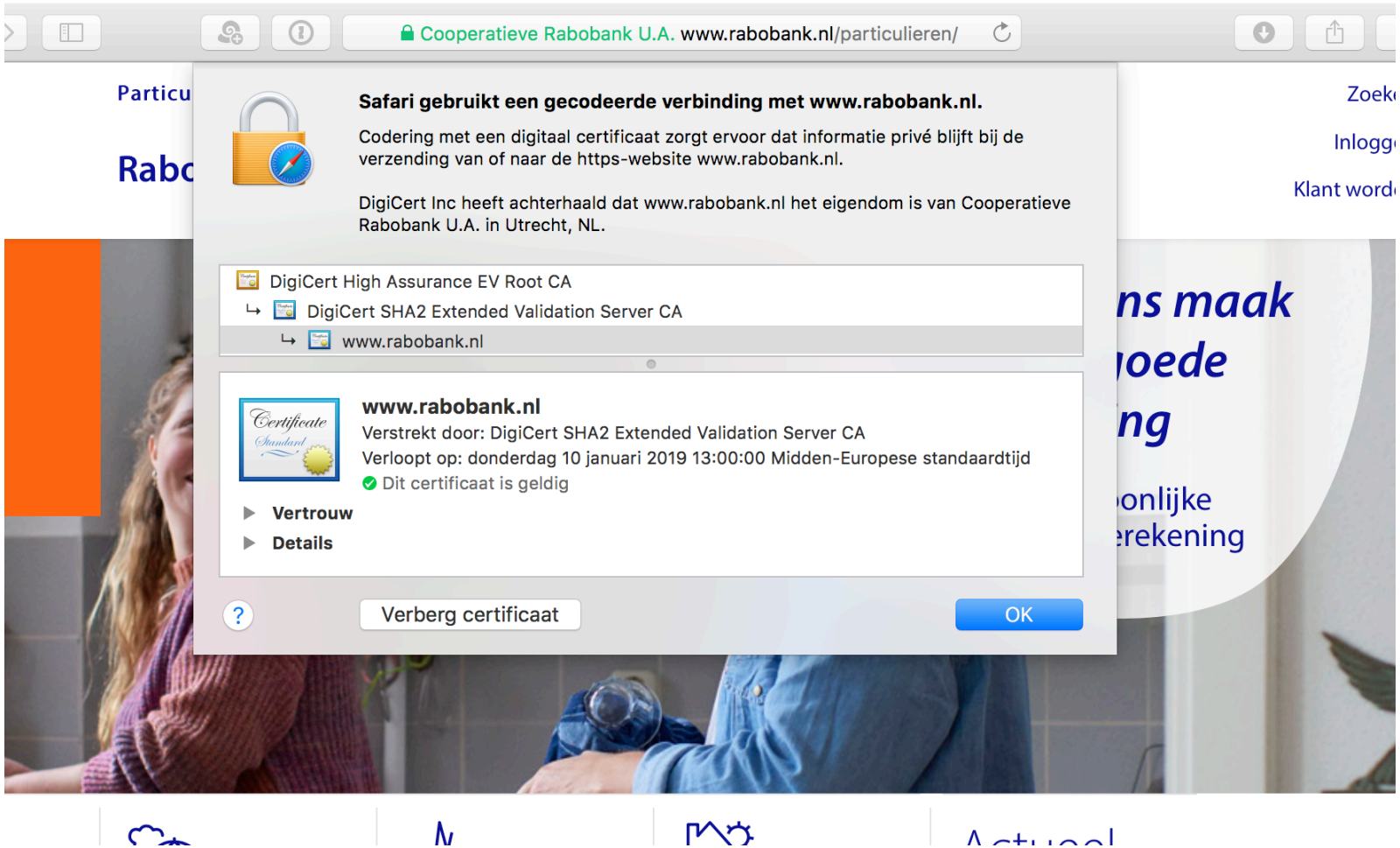
Authenticatie

- Man in the middle
- Weet je wel zeker dat je met de server van de bank verbinding maakt?
- Een certificaat garandeert dat je verbinding hebt met de server die bij het domein hoort
- Certificaat is dus een soort paspoort voor websites



Uitgevers

- Certificaat wordt uitgegeven met een waarmerk van de certificaatuitgever / certificaatautoriteit.
- Deze uitgever heeft zelf ook een certificaat om te garanderen dat de ondertekening van het eerste certificaat écht van deze certificaatautoriteit komt. Het certificaat van de uitgever is ondertekend door een hogere certificaatautoriteit.
- Ook die ondertekening kan worden gecontroleerd, etc… Totdat je op een certificaat uitkomt dat aan de top staat.
- Terug te voeren op slechts een aantal stam(=root)certificaten. Je browser heeft hier beschikking over.



Certificaten inspecteren

rabobank.nl
triodos.nl
tv.e

Malware

- Virus heeft mens nodig om te verspreiden
- Worm verspreidt zich zonder tussenkomst van mens
- Trojaans paard lijkt iets onschuldigs, maar is malware
- Ransomware brengt schade aan (bijv. encryptie van bestanden) en vraagt losgeld om het weer op te lossen.

Wachtwoorden

- Hoe sterk is jouw wachtwoord?
  www.passwordmeter.com
  tip: vul geen wachtwoorden in die je daadwerkelijk gebruikt
- Wat is een veilig wachtwoord?
- Bruteforce aanval
- Woordenboek aanval

Wachtwoord kraken

- Verschillende manieren:
  - Brute force: één voor één alle mogelijkheden uitproberen
  - Dictionary attack: één voor één een lijst van meest gebruikte wachtwoorden uitproberen. (Met daarbij de mogelijkheid om combinaties / variaties mee te nemen, zoals ‘password’ en ‘p@ssw0rd’.
    Bij gerichte aanval op een persoon: probeer gegevens te achterhalen, zoals geboortedata en namen van geliefden etc. Om zo een persoonlijke woordenboek samen te stellen.
  - Of: social engineering / pretexting -> contact met iemand leggen en informatie proberen te ontfutselen

Aantal mogelijkheden

- De sterkte van een wachtwoord is onder andere afhankelijk van hoeveel mogelijkheden er zijn. Succes van brute force is hierop gebaseerd

- Aantal mogelijkheden bereken je door aantal mogelijke tekens te verheffen tot de macht van het aantal posities

- Bijv wachtwoord van 8 tekens bestaan uit alleen kleine letters: 26^8 = 208827064576 mogelijkheden