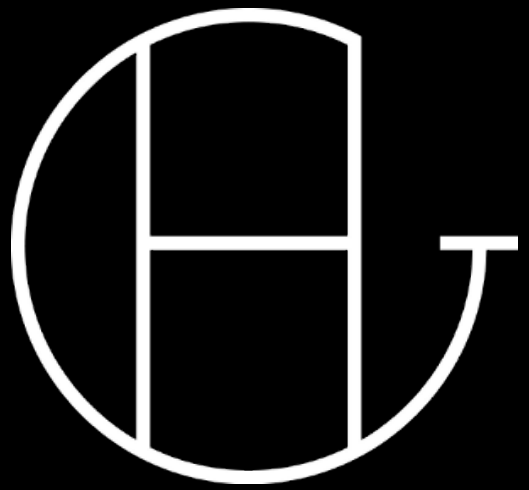


HoGent

BEDRIJF
EN
ORGANISATIE

Coding For Dummies

Jens Buysse

Inhoud

De eerste codes

When Cryptography is outlawed, bayl bh-gynjf jvyy unir cevinpl

– John Perry Barlow

Cryptografie

Het woord cryptografie betekent letterlijk geheim schrijven of verborgen schrijven, het is voortgekomen uit de 2 griekse woorden

- kruptos en
- graphein

wat samen geheim schrijven betekent.

De eerste codes

Zowel de Romeinen als de Grieken verdiepten zich in de grondbeginselen van cryptografie.

- Optische signalen m.b.h.v. toortsen
- vlaggen
- spiegels
- ...

De eerste codes

Polybius

Code ontwikkeld door Griekse militair.

$$\begin{bmatrix} & 1 & 2 & 3 & 4 & 5 \\ 1 & A & B & C & D & E \\ 2 & F & G & H & I & J \\ 3 & K & L & M & N & O \\ 4 & P & Q & R & S & T \\ 5 & V & W & X & Y & Z \end{bmatrix}$$

Wat betekent volgend geheimschrift?

$$\begin{bmatrix} 12 & 53 & 34 & 54 & 15 & 43 & 51 & 12 & 11 & 15 \\ 53 & 34 & 44 & 54 & 32 & 51 & 21 & 53 & 23 & 41 \end{bmatrix}$$

Polybius

Er werden twee reeksen van fakkels opgesteld:

1. Eerste 5 fakkels duiden de rij aan
2. Tweede 5 fakkels duiden de kolom aan

Aenas' Telegraaf

Aenas' Telegraaf

1. Partij A heft een brandende fakkel
2. Partij B heft ten antwoord ook een brandende fakkel
3. Partij A laat fakkel zaken en kranen worden open gezet
4. Partij A heft opnieuw brandende fakkel op zodat kranen gesloten kunnen worden.

Caesarscode

Elke letter wordt vervangen door de letter die een afgesproken aantal plaatsen (bv. 3) verder in het alfabet staat.

Code

EDG LV D SODQ ZKLFK FDQQRW EHDU D FKDQJH

Caesarscode - zwaktes

Wat zijn de zwaktes van deze codering en hoe zou je deze aanpakken?

Caesarscode - zwaktes

Wat zijn de zwaktes van deze codering en hoe zou je deze aanpakken?

- Biedt slechts 25 mogelijkheden tot versleuteling. (Computer kan dit makkelijk kraken)
- De letter E komt heel erg vaak voor in de taal. Door te tellen welke letter het meest voorkomt kan je al goed raden wat de E zal zijn.
- Je weet ook al wat de woorden zijn.

Code

ROHXD VDBCK ANJTC QNUJF MXRCC XBNRI NYXFN ARWJU UXCQN ALJBN BXKBN AENRC

Scytale

Code

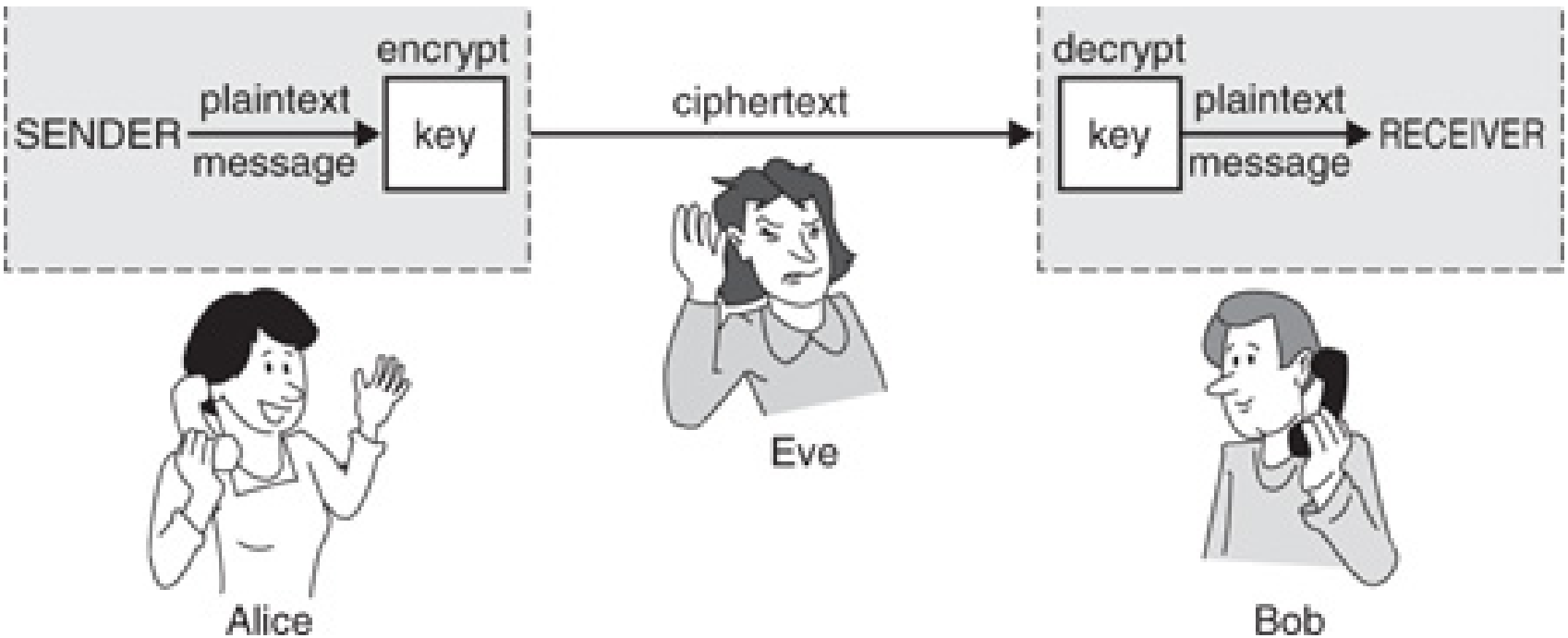
ANACD DEIOR SUTWB AOTIR FNSUE ELNTF EHRMA IYNE

lets formeler

Cryptography shifts the balance of power from those with a monopoly on violence to those who comprehend mathematics and security design.

Jacob Appelbaum

Adam, Alice & Eve



Cryptografieindeling

Symmetrisch Wanneer de sleutel om te versleutelen en ontsleutelen dezelfde is. Versleuteling kan enkel veilig gebeuren wanneer er een veilige sleuteluitwisseling tussen Alice en Bob gebeurd is.

Assymetrisch Of ook publieke sleutel cryptografie waarbij het versleutelen en ontsleutelen met een verschillende sleutel moet.

We merken op dat hedendaagse versleutelingsmechanismen vaak een gelaagde combinatie van bovengenoemde types zijn.

Enkele definities

Plaintext / Cleartext Het ongecodeerde bericht.

Encryption de codering van de plaintext

Ciphertext Dit is de uiteindelijke tekst, in versleutelde vorm. Bij een goed gecodeerde tekst is de ciphertext een onbegrijpelijke boodschap, waaruit onbevoegden praktisch onmogelijk de plaintext kunnen halen.

Decryption De decryption is de stap die de ontvanger uitvoert om het originele bericht weer uit de ciphertext te halen.

Key De key is de sleutel die je nodig hebt om een ciphertext te decoderen.

Cryptanalysis Dit begrip houdt het kraken van een gecodeerde tekst in.

Cryptology Cryptologie is een net iets minder ruim begrip dan Cryptografie. Bij cryptologie wordt namelijk alleen de wiskundige kant van de cryptografie bestudeerd.

Kraakpogingen - Kerckhoffs' principes

1. Het systeem dient, zelfs als het in theorie niet onbreekbaar is, in de praktijk onbreekbaar te zijn.

Kraakpogingen - Kerckhoffs' principes

1. Het systeem dient, zelfs als het in theorie niet onbreekbaar is, in de praktijk onbreekbaar te zijn.
2. Het ontwerp van het systeem behoort niet geheim te hoeven zijn en dient, indien gecompromitteerd, de correspondenten niet te kunnen schaden.

Kraakpogingen - Kerckhoffs' principes

1. Het systeem dient, zelfs als het in theorie niet onbreekbaar is, in de praktijk onbreekbaar te zijn.
2. Het ontwerp van het systeem behoort niet geheim te hoeven zijn en dient, indien gecompromitteerd, de correspondenten niet te kunnen schaden.
3. De sleutel moet onthoudbaar zijn zonder notities en dient makkelijk veranderd te kunnen worden.

Kraakpogingen - Kerckhoffs' principes

1. Het systeem dient, zelfs als het in theorie niet onbreekbaar is, in de praktijk onbreekbaar te zijn.
2. Het ontwerp van het systeem behoort niet geheim te hoeven zijn en dient, indien gecompromitteerd, de correspondenten niet te kunnen schaden.
3. De sleutel moet onthoudbaar zijn zonder notities en dient makkelijk veranderd te kunnen worden.
4. De cryptogrammen moeten overgebracht kunnen worden door middel van telegrafie.

Kraakpogingen - Kerckhoffs' principes

1. Het systeem dient, zelfs als het in theorie niet onbreekbaar is, in de praktijk onbreekbaar te zijn.
2. Het ontwerp van het systeem behoort niet geheim te hoeven zijn en dient, indien gecompromitteerd, de correspondenten niet te kunnen schaden.
3. De sleutel moet onthoudbaar zijn zonder notities en dient makkelijk veranderd te kunnen worden.
4. De cryptogrammen moeten overgebracht kunnen worden door middel van telegrafie.
5. Het apparaat of de documenten dienen draagbaar te zijn en te kunnen worden bediend door een enkel persoon.

Kraakpogingen - Kerckhoffs' principes

1. Het systeem dient, zelfs als het in theorie niet onbreekbaar is, in de praktijk onbreekbaar te zijn.
2. Het ontwerp van het systeem behoort niet geheim te hoeven zijn en dient, indien gecompromitteerd, de correspondenten niet te kunnen schaden.
3. De sleutel moet onthoudbaar zijn zonder notities en dient makkelijk veranderd te kunnen worden.
4. De cryptogrammen moeten overgebracht kunnen worden door middel van telegrafie.
5. Het apparaat of de documenten dienen draagbaar te zijn en te kunnen worden bediend door een enkel persoon.
6. Het systeem dient gemakkelijk te zijn, niet onderhevig aan kennis van allerlei regels of aan mentale inspanning

Kraakpogingen - Kerckhoffs' principes

1. Het systeem dient, zelfs als het in theorie niet onbreekbaar is, in de praktijk onbreekbaar te zijn.
2. Het ontwerp van het systeem behoort niet geheim te hoeven zijn en dient, indien gecompromitteerd, de correspondenten niet te kunnen schaden.
3. De sleutel moet onthoudbaar zijn zonder notities en dient makkelijk veranderd te kunnen worden.
4. De cryptogrammen moeten overgebracht kunnen worden door middel van telegrafie.
5. Het apparaat of de documenten dienen draagbaar te zijn en te kunnen worden bediend door een enkel persoon.
6. Het systeem dient gemakkelijk te zijn, niet onderhevig aan kennis van allerlei regels of aan mentale inspanning

Belangrijk: *principe van Kerckhoffs*: de veiligheid van een cryptografisch systeem mag niet van de geheimhouding van het versleutelingssysteem maar slechts van de geheimhouding van de sleutel afhangen.

Kraakpoging - Brute Force

Brute force (Engels voor "brute kracht") is het gebruik van rekenkracht om een probleem op te lossen met een computer zonder gebruik te maken van algoritmen of heuristieken

- De methode bestaat uit het botweg uitproberen van alle mogelijke opties, net zo lang tot er een gevonden is die overeenkomt met de gewenste invoer.

Combo Attack

Gebruik een woordenboek en plak de verschillende woorden tezamen.

- dictionary1.txt & dictionary2.txt
- pass $\rightarrow$ password, passpass, passlion
- word $\rightarrow$ wordpass, wordword, wordlion
- lion $\rightarrow$ lionpass, lionword, lionlion

Combo Attack

Combo attack, maar met de mogelijkheid een willekeurige reeks letters toe te voegen

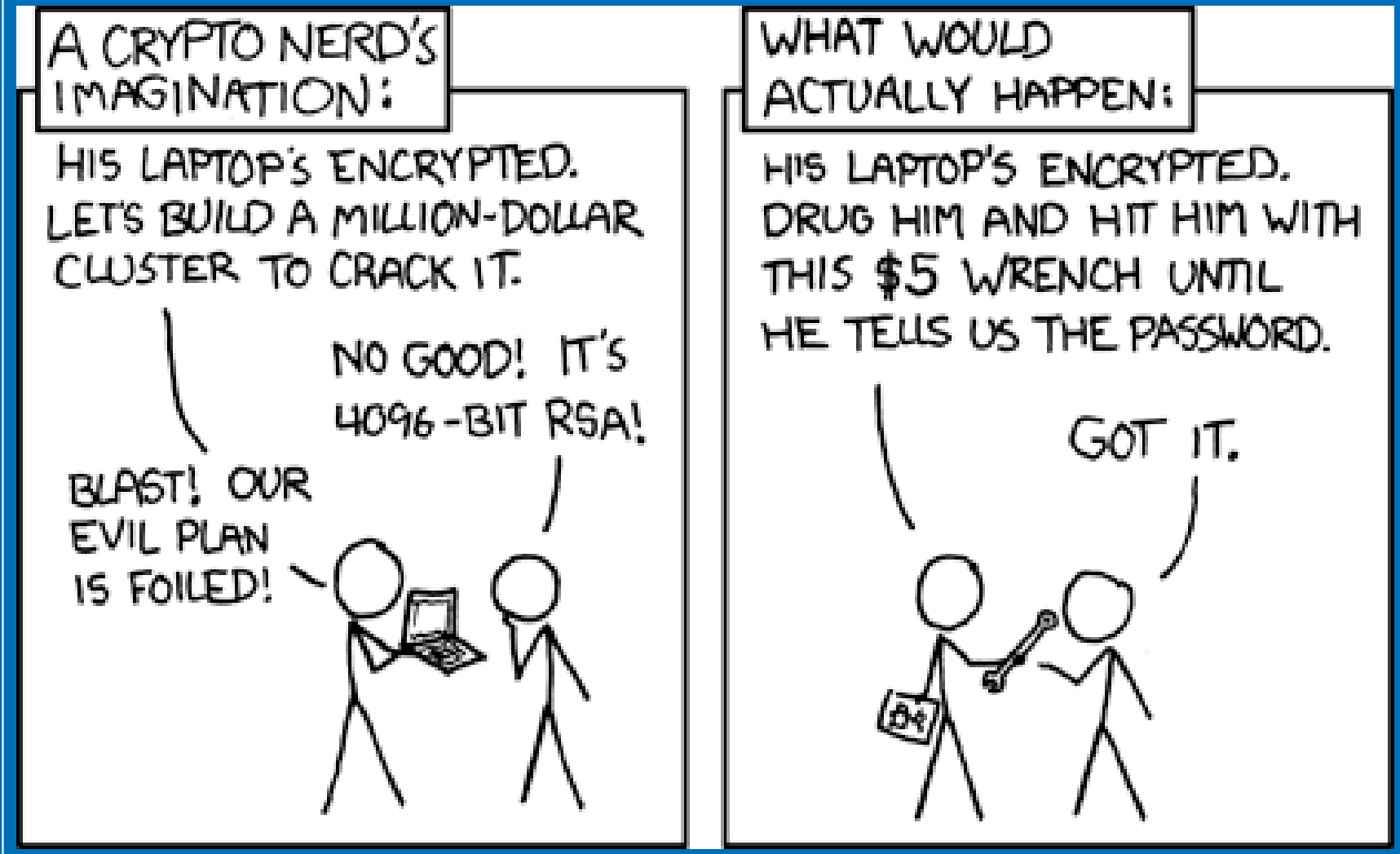
- dictionary.txt & abcde
- pass $\rightarrow$ passAbc, passBcd, passCde
- word $\rightarrow$ wordAbc, wordBcd, wordCde
- lion $\rightarrow$ lionAbc, lionBcd, lionCde

Use Case: Wordpress websites

Als je gebruikt maakt van Wordpress ben je kwetsbaar voor Brute Force attacks.
Je kan hiertegen een aantal eenvoudige maatregelen gebruiken:

1. Sterke paswoorden gebruiken
2. De admingebruikersnaam veranderen
3. Het aantal loginpogingen beperken
4. Loginpagina anders noemen
5. IP adressen die toegang hebben beperken
6. CAPTCHA toevoegen

RSA


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

RSA

——BEGIN PUBLIC KEY——

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvUWEGue
PMihBxG8/mhi1z9YdCXEDk01iqLcYEKa4uPfPao0DAU2/4hSkWu
JCgBkAzJns8hz7DKskdRrTnhG1rcomyLFz07GFq1qkmpc6bL1UW
UNsdIOtu0CsgbtdeFW5OMJhezljf/jvuYRpE+eNPwHmg0233JvN
TVQ2ZNUO9eXX7gt1qYKZiHR3warYYE+7ro6BOwY3pBOG8iIm3zj
u2ioICGFH/hd9Jd19+mZwWneccYv89W1eSyPYg5yBWIIYLSFZA9
imIO0Xe3/ifRQyDjaE5YbTQt6/CkBYmObp009Exp3QwPnpYLTKM
zhjfgk+5Bg3O2wVVX+1ny7QqLSHrQIDAQAB

——END PUBLIC KEY——

RSA

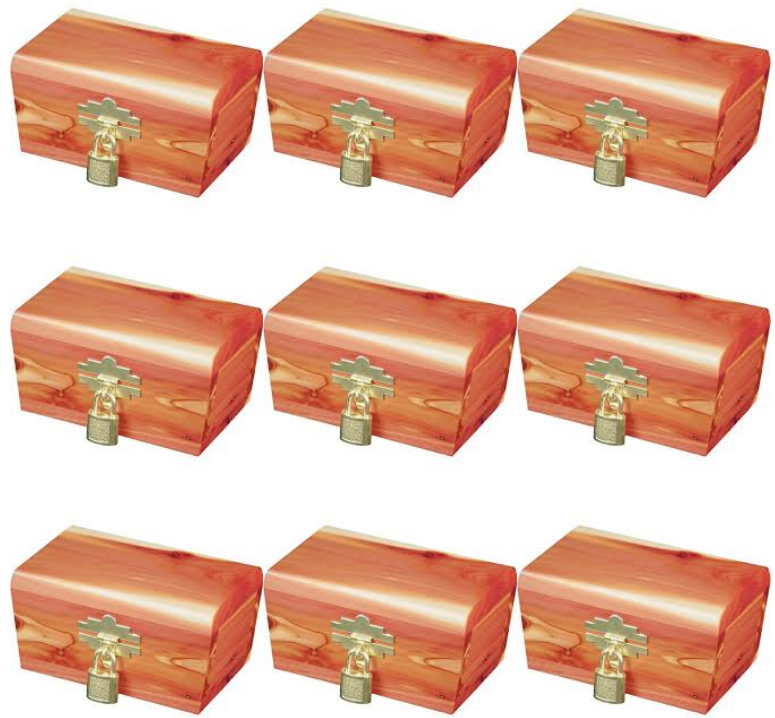
RSA

RSA

RSA

RSA

RSA



Modulo rekenen

Stel dat het op een moment 20 uur is , en je telt daar 7 uur bij op. Dan zou het volgens gewone rekenmethodes dus $20 + 7 = 27$ uur moeten zijn.
Maar niemand noemt dat 27 uur, iedereen zegt 3 uur. Dat komt natuurlijk omdat het de volgende dag is geworden en die 24 uur van de vorige dag interesseren ons niet zoveel meer.

Modulo rekenen

Zij n n een natuurlijk getal $\neq 0$, dan heten de twee gehele getallen a en b congruent modulo n, genoteerd:

$$a \equiv b \pmod{n}$$

als hun verschil $a - b$ een geheel veelvoud is van n.
Het getal n wordt de modulus genoemd.

Voorbeelden modulo rekenen

$$26 \pmod 8 =$$

Voorbeelden modulo rekenen

$$\begin{aligned} 26 \pmod 8 &= 2 \\ -13 \pmod 8 &= \end{aligned} \tag{1}$$

Voorbeelden modulo rekenen

$$26 \pmod 8 = 2 \tag{1}$$

$$-13 \pmod 8 = 3 \tag{2}$$

$$257 \pmod 8 =$$

Voorbeelden modulo rekenen

$$26 \pmod 8 = 2 \tag{1}$$
$$-13 \pmod 8 = 3 \tag{2}$$
$$257 \pmod 8 = 1 \tag{3}$$

Andere notatie

$$26 \pmod 8 = 2 + k \times 8 \tag{4}$$

$$-13 \pmod 8 = 3 + k \times 8 \tag{5}$$

$$257 \pmod 8 = 1 + k \times 8 \tag{6}$$

Modulo Rekenregels$_1$

$$a \pmod m + b \pmod m = (a+b) \pmod m$$

Modulo Rekenregels$_2$

$$a \pmod{m} \times b \pmod{m} = (a \times b) \pmod{m}$$

Modulo Rekenregels$_3$

$$(a \pmod m)^n = a^n \pmod m$$

Toepassing bankrekeningen - Nederland

$$c_1c_2c_3c_4c_5c_6c_7c_8c_9$$

Nu is c_9 zo gekozen dat, als je dit getal $\pmod{11}$ neemt, er 0 uitkomt.

Toepassing bankrekeningen - Nederland

$$45824365c_9$$

bepaal

$$9 \times 4 + 8 \times 5 + \cdots + 2 \times 5$$

Kies c_9 zodat $\sum_i^9 i \times c_i \pmod{11} = 0$

Toepassing bankrekeningen - Nederland

$$45824365c_9$$

bepaal

$$9 \times 4 + 8 \times 5 + \cdots + 2 \times 5$$

Kies c_9 zodat $\sum_i^9 i \times c_i \pmod{11} = 0$
Als de som 204 is dan moet $c_9 = 5$

RSA

Omgekeerde functie

Men verstaat onder de inverse van een variabele x ten opzichte van een bepaalde binaire bewerking het getal x^{-1}, waarvoor het resultaat van de bewerking toegepast op x en de inverse het neutrale element van die bewerking oplevert.

$$7 \times 328 = 2296$$

Dit is eigenlijk een versleuteling van 7.

$$2296 * \times \frac{1}{328} = 7$$

of

$$328 \times \frac{1}{328} = 1$$

RSA Algoritme : stap 1

Neem 2 grote priemgetallen (100 cijfers of meer). Laten we die getallen p_1 en p_2 noemen.

Voorbeeld

$$p_1 = 5 \wedge p_2 = 7$$

RSA Algoritme : stap 2

Vermenigvuldig p_1 en p_2.

$$m = p_1 \times p_2$$

Dit noemen we de modulus en vormt een deel van de publieke sleutel.

Voorbeeld

$$p_1 = 5 \wedge p_2 = 7$$

$$7 \times 5 = 35 = m$$

RSA Algoritme : stap 3

Bereken een getal $\Phi =$ het aantal getallen kleiner dan m dat geen priemfactor met m gemeenschappelijk heeft

Voorbeeld

Priemfactoren?

Priemgetallen zijn de bouwstenen van alle andere getallen: elk getal kan opgedeeld worden in priemfactoren.
Bv.

$$12 = 4 \times 3 = 2 \times 2 \times 3 = 2^2 \times 3$$

RSA Algoritme : stap 3

Bereken een getal $\Phi =$ het aantal getallen kleiner dan m dat geen priemfactor met m gemeenschappelijk heeft

Voorbeeld

$$p_1 = 5 \wedge p_2 = 7$$

$$7 \times 5 = 35 = m$$

m is opgebouwd uit de priemfactoren 5 en 7. Dus alle getallen onder de 35 waar een 5 of een 7 inzit vallen af. Dat zijn 5, 10, 15, 20, 25, 30, 35, 7, 14, 21, 28 dus dat zijn er 11. Dus blijven er 35 - 11 $=$ 24 getallen over, dus $\Phi = 24$.

RSA Algoritme : stap 3

Bereken een getal $\Phi =$ het aantal getallen kleiner dan m dat geen priemfactor met m gemeenschappelijk heeft

Voorbeeld

$$p_1 = 5 \wedge p_2 = 7$$

$$7 \times 5 = 35 = m$$

$$\Phi = \Phi(p_1.p_2) = (p_1 - 1) \times (p_2 - 1)$$

RSA Algoritme : stap 3

- Alle getallen uit de tafel van p_1 vallen af, dat zijn er p_2
- Alle getallen uit de tafel van p_2 vallen af, dat zijn er p_1
- Maar nu hebben we het getal $p_1 \times p_2$ dubbel meegeteld, dus er moet weer eentje bij.

Dan blijft over

$$(p_1 \times p_2) - p_1 - p_2 + 1 = (p_1 - 1) \times (p_2 - 1)$$

RSA Algoritme : stap 3

Bereken een getal $\Phi =$ het aantal getallen kleiner dan m dat geen priemfactor met m gemeenschappelijk heeft

Voorbeeld

$$p_1 = 5 \wedge p_2 = 7$$

$$7 \times 5 = 35 = m$$

$$\Phi(35) = 4 \times 6 = 24$$

RSA Algoritme : stap 4

Kies een nieuw getal e kleiner $< m$, waarvoor geldt dat dat getal geen deler met Φ gemeenschappelijk mag hebben. Dan is e uit allemaal andere priemfactoren opgebouwd dan Φ.

Voorbeeld

$$p_1 = 5 \wedge p_2 = 7$$

$$7 \times 5 = 35 = m$$

$$\Phi(35) = 4 \times 6 = 24$$

$$\Phi(35) = 2.2.2.3 \rightarrow e \in 5, 7, 25$$

Stel $e = 7$.

RSA Algoritme : stap 4

Je maakt deze getallen m en e openbaar. Zij vormen samen jouw publieke sleutel.

Voorbeeld

$$p_1 = 5 \wedge p_2 = 7$$

$$7 \times 5 = 35 = m$$

$$\Phi(35) = 4 \times 6 = 24$$

$$\Phi(35) = 2.2.2.3 \rightarrow e \in 5, 7, 25$$

Stel $e = 7$.
Versleuteling is:

$$G = B^e \pmod{m}$$

RSA Algoritme : versleutelingsvoorbeeld

- Stel A $= 01$, B $= 02$, C $= 03$ ....
- Stel dat je het miniberichtje B $=$ "12"wilt versturen (de letter L dus).
- Dan bereken je dus $G = 12^7 \pmod{35} = 33$
- Je verstuurt het geheime bericht $G = 33$.

RSA Algoritme : stap 5

Creëer d waarvoor geldt:
$e \times d = 1 \pmod{\Phi}$.
Ontsleuteling is

$$B = 33^7 \pmod{35}$$

Voorbeeld

$$B = 33^7 \pmod{35}$$

$$33^7 \pmod{35}$$

$$33^4 \pmod{35} \times 33^3 \pmod{35}$$

$$51 \times 27 \pmod{35}$$

$$1377 \pmod{35} = 12$$

Waarom werkt dit: Kleine stelling van Fermat

Het komt allemaal omdat de bewerking "tot-de-macht-d"de inverse is van "tot-de-macht-e"(beiden mod m).
Voor elk priemgetal p en elk getal a dat geen priemfactoren p heeft geldt:

$$a^p = a \pmod{p}$$

Voorbeeld: $67 = 279936 = 6 + 279930 = 6 + 7 \times 39990 = 6(mod 7)$

Waarom is dit moeilijk te kraken

- RSA is zo moeilijk te ontcijferen omdat het haast niet te doen is om van een enorm getal m te vinden uit welke twee priemgetallen m is opgebouwd. Als m uit veel meer priemfactoren zou bestaan zou dat veel makkelijker te vinden zijn, want zodra je er dan eentje hebt gevonden kun je m daardoor delen en wordt het snel kleiner.
- Verder is RSA ondanks die enorme getallen toch makkelijk te gebruiken omdat machtsverheffen bij modulorekenen makkelijk is.
- Het bericht B dat je wilt versturen mag niet groter zijn dan e. Als dat wel zo is, dan moet je het eerst in kleinere stukken hakken en die 1 voor 1 doorsturen.

Samenvattend

1. Kies grote priemgetallen p en q (minstens 100 cijfers elk).
2. Bepaal de modulus $m = p \times q$.
3. Bereken $\Phi = (p-1)(q-1)$.
4. Kies een vercijferexponent e waarvoor $ggd(e, \Phi) = 1$.
5. Bereken d zo, dat $e \times d = 1 \pmod{\Phi}$.
6. Maak de getallen m en e bekend. Samen vormen die de openbare sleutel.
7. Houd d geheim. Dat is de geheime sleutel.
8. Vercijferen:$E(x) = x^e \pmod{m}$
9. Ontcijferen: $D(y) = y^d \pmod{m}$

Voorbeeld

Als priemgetallen nemen we $p = 74471$ en $q = 98773$.

Voorbeeld

Als priemgetallen nemen we p = 74471 en q = 98773. De modulus m = p x q is dan 7355724083. Het getal n = (p 1)(q 1) is nu 7355550840, en voor e nemen we 619. Het algoritme van Euclides leert ons dat e inderdaad geen delers met n gemeen heeft, en bovendien dat de inverse d van e gelijk is aan 4313513659. Neem nu als boodschap PRIEM. In cijfers wordt dat x = 1618090513. Vercijferen levert: