HoGent

BEDRIJF EN ORGANISATIE

Coding For Dummies

Jens Buysse / Stijn Lievens

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’.
We herkennen hierin 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

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.
5. Stand van het water duidt de verzonden boodschap aan.

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.
5. Stand van het water duidt de verzonden boodschap aan.

Nadeel: Slechts een beperkt aantal boodschappen kon verzonden worden.

Polybius

Code ontwikkeld door Griekse militair.

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

Polybius

Code ontwikkeld door Griekse militair.

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

Merk op: er is geen apart teken voor U (identiek aan V)

Polybius

Code ontwikkeld door Griekse militair.

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

Merk op: er is geen apart teken voor U (identiek aan V)
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 kolom aan
2. Tweede 5 fakkels duiden de rij aan

Polybius

Er werden twee reeksen van fakkels opgesteld:

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

Hoe snel is dit systeem?

Polybius

Er werden twee reeksen van fakkels opgesteld:

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

Hoe snel is dit systeem?
Antwoord: studenten uit Aken in jaren '80: 8 letters/minuut.

Polybius

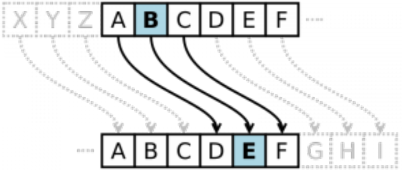
Er werden twee reeksen van fakkels opgesteld:

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

Hoe snel is dit systeem?
Antwoord: studenten uit Aken in jaren '80: 8 letters/minuut.Als 1 letter gelijk is aan 8 bits: 64 bits/minuut

Caesarscode

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



Na de 'Z' komt opnieuw de 'A'.

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

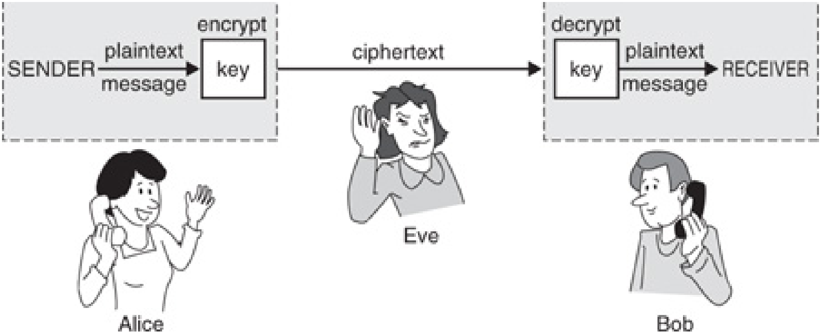
ANACD DEIOR SUTWB AOTIR FNSUE ELNTF EHRMA IYNE

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

Alice, Bob & Eve



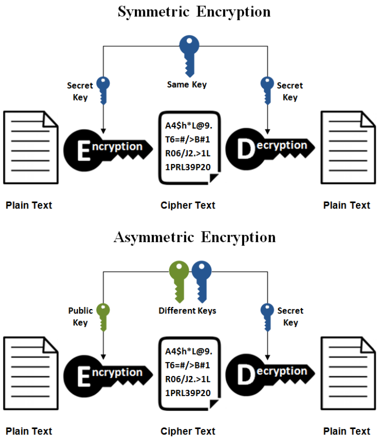
Cryptografieindeling

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.

Asymmetrisch Of ook **publieke sleutel** cryptografie waarbij het versleutelen en ontsleutelen met een verschillende sleutel moet gebeuren.

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

Symmetrische vs Asymmetrische Encryptie



Enkele definities

Plaintext / Cleartext Het ongecodeerde bericht.

Encryption Het proces van het coderen 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.

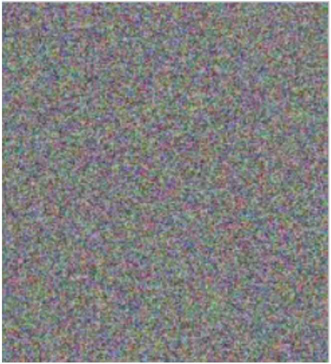
Decryption De decryption is de stap die de ontvanger uitvoert om het originele bericht weer uit de ciphertext te halen.

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

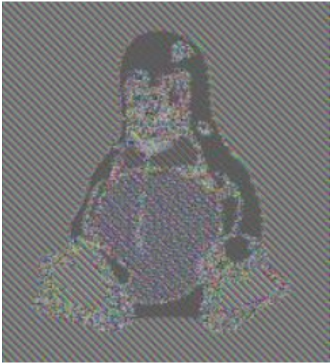
Cryptanalysis Dit begrip houdt het kraken van een gecodeerde tekst in.

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

Voorbeeld Plaintext en Ciphertext



Voorbeeld Plaintext en Zwakke Ciphertext



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 m.a.w. uit het botweg uitproberen van alle mogelijke mogelijkheden (sleutels), tot er een gevonden is die overeenkomt met de gewenste uitvoer.

Combo Attack

Gebruik een woordenboek en plak de verschillende woorden tezamen.

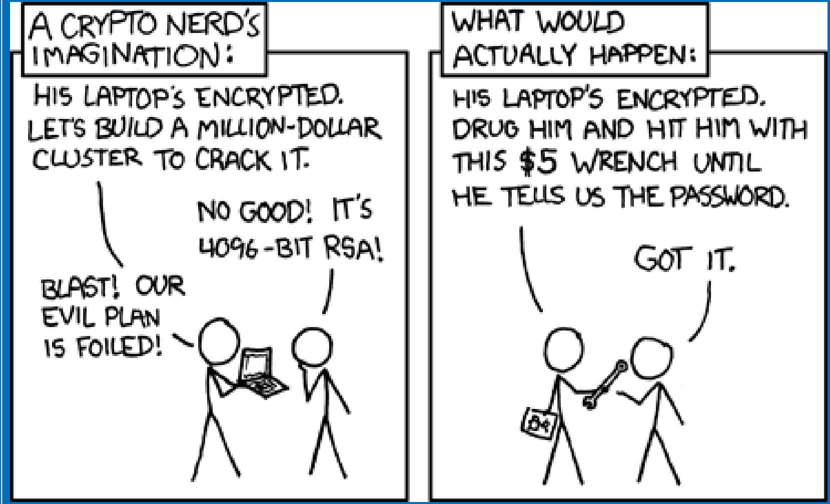
- dictionary1.txt & dictionary2.txt
- pass → password, passpass, passlion
- word → wordpass, wordword, wordlion
- lion → lionpass, lionword, lionlion

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

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
UNsdIOtu0CsgbtdeFW5OMJhezIjf/jvuYRpE+eNPwHmg0233JvN
TVQ2ZNUO9eXX7gt1qYKZiHR3warYYE+7ro6BOwY3pBOG8iIm3zj
u2ioICGFH/hd9Jd19+mZwWneccYv89W1eSyPYg5yBWIIYLSFZA9
imIO0Xe3/ifRQyDjaE5YbTQt6/CkBYmObp009Exp3QwPnpYLTKM
zhjfgk+5Bg3O2wVVX+1ny7QqLSHrQIDAQAB
-----END PUBLIC KEY-----

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 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.
We noteren

$$a \pmod{n}$$

als het getal tussen 0 en $n-1$ waar a congruent mee is modulo n.

Voorbeelden modulo rekenen

$$26 \pmod 8 \quad =$$

Voorbeelden modulo rekenen

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

Voorbeelden modulo rekenen

$$\begin{aligned} 26 \pmod 8 &= 2 \\ -13 \pmod 8 &= 3 \\ 257 \pmod 8 &= \end{aligned}$$

Voorbeelden modulo rekenen

$$\begin{aligned} 26 &\pmod 8 &= 2 \\ -13 &\pmod 8 &= 3 \\ 257 &\pmod 8 &= 1 \end{aligned}$$

Modulo Rekenregels: Optelling

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

Voorbeeld: Stel $a = 23$, $b = -10$ en $n = 8$.

Modulo Rekenregels: Optelling

$$a \pmod{n} + b \pmod{n} = (a+b) \pmod{n}$$

Voorbeeld: Stel $a = 23$, $b = -10$ en $n = 8$.

- We berekenen het rechterlid: $a + b = 13$ zodat $13 \pmod{8} = 5$.

Modulo Rekenregels: Optelling

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

Voorbeeld: Stel $a = 23$, $b = -10$ en $n = 8$.

- We berekenen het rechterlid: $a + b = 13$ zodat $13 \pmod 8 = 5$.
- We berekenen het linkerlid:

Modulo Rekenregels: Optelling

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

Voorbeeld: Stel $a = 23$, $b = -10$ en $n = 8$.

- We berekenen het rechterlid: $a + b = 13$ zodat $13 \pmod 8 = 5$.
- We berekenen het linkerlid:
  - $a \pmod n = 23 \pmod 8 = 7$

Modulo Rekenregels: Optelling

$$a \pmod{n} + b \pmod{n} = (a+b) \pmod{n}$$

Voorbeeld: Stel $a = 23$, $b = -10$ en $n = 8$.

- We berekenen het rechterlid: $a + b = 13$ zodat $13 \pmod{8} = 5$.
- We berekenen het linkerlid:
  - $a \pmod{n} = 23 \pmod{8} = 7$
  - $b \pmod{n} = -10 \pmod{8} = 6$

Modulo Rekenregels: Optelling

$$a \pmod{n} + b \pmod{n} = (a+b) \pmod{n}$$

Voorbeeld: Stel $a = 23$, $b = -10$ en $n = 8$.

- We berekenen het rechterlid: $a + b = 13$ zodat $13 \pmod{8} = 5$.
- We berekenen het linkerlid:
  - $a \pmod{n} = 23 \pmod{8} = 7$
  - $b \pmod{n} = -10 \pmod{8} = 6$
  - $7 + 6 = 13$ en $13 \pmod{8} = 5$

Modulo Rekenregels: Vermenigvuldiging

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

Voorbeeld: Stel $a = 23$, $b = -10$ en $n = 8$.

Modulo Rekenregels: Vermenigvuldiging

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

Voorbeeld: Stel $a = 23$, $b = -10$ en $n = 8$.

- We berekenen het rechterlid: $a \times b = -230$ zodat $-230 \pmod{8} = 2$ (want $-230 = -29 \times 8 + 2$)

Modulo Rekenregels: Vermenigvuldiging

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

Voorbeeld: Stel $a = 23$, $b = -10$ en $n = 8$.

- We berekenen het rechterlid: $a \times b = -230$ zodat $-230 \pmod{8} = 2$ (want $-230 = -29 \times 8 + 2$)
- We berekenen het linkerlid:

Modulo Rekenregels: Vermenigvuldiging

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

Voorbeeld: Stel $a = 23$, $b = -10$ en $n = 8$.

- We berekenen het rechterlid: $a \times b = -230$ zodat $-230 \pmod{8} = 2$ (want $-230 = -29 \times 8 + 2$)
- We berekenen het linkerlid:
  - $a \pmod{n} = 23 \pmod{8} = 7$

Modulo Rekenregels: Vermenigvuldiging

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

Voorbeeld: Stel $a = 23$, $b = -10$ en $n = 8$.

- We berekenen het rechterlid: $a \times b = -230$ zodat $-230 \pmod{8} = 2$ (want $-230 = -29 \times 8 + 2$)
- We berekenen het linkerlid:
  - $a \pmod{n} = 23 \pmod{8} = 7$
  - $b \pmod{n} = -10 \pmod{8} = 6$

Modulo Rekenregels: Vermenigvuldiging

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

Voorbeeld: Stel $a = 23$, $b = -10$ en $n = 8$.

- We berekenen het rechterlid: $a \times b = -230$ zodat $-230 \pmod{8} = 2$ (want $-230 = -29 \times 8 + 2$)
- We berekenen het linkerlid:
  - $a \pmod{n} = 23 \pmod{8} = 7$
  - $b \pmod{n} = -10 \pmod{8} = 6$
  - $7 \times 6 = 42$ en $42 \pmod{8} = 2$

Modulo Rekenregels: Machtsverheffing

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

Voorbeeld: Stel $a = 23$, $m = 5$ en $n = 8$.

Modulo Rekenregels: Machtsverheffing

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

Voorbeeld: Stel $a = 23$, $m = 5$ en $n = 8$.

- We berekenen het rechterlid: $23^5 = 6436343$ zodat $6436343 \pmod 8 = 7$ (want $6436343 = 804542 \times 8 + 7$)

Modulo Rekenregels: Machtsverheffing

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

Voorbeeld: Stel $a = 23$, $m = 5$ en $n = 8$.

- We berekenen het rechterlid: $23^5 = 6436343$ zodat $6436343 \pmod 8 = 7$ (want $6436343 = 804542 \times 8 + 7$)
- We berekenen het linkerlid:

Modulo Rekenregels: Machtsverheffing

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

Voorbeeld: Stel $a = 23$, $m = 5$ en $n = 8$.

- We berekenen het rechterlid: $23^5 = 6436343$ zodat $6436343 \pmod 8 = 7$ (want $6436343 = 804542 \times 8 + 7$)
- We berekenen het linkerlid:
  - $a \pmod n = 23 \pmod 8 = 7$

Modulo Rekenregels: Machtsverheffing

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

Voorbeeld: Stel $a = 23$, $m = 5$ en $n = 8$.

- We berekenen het rechterlid: $23^5 = 6436343$ zodat $6436343 \pmod 8 = 7$ (want $6436343 = 804542 \times 8 + 7$)
- We berekenen het linkerlid:
  - $a \pmod n = 23 \pmod 8 = 7$
  - $7^5 = 16807$

Modulo Rekenregels: Machtsverheffing

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

Voorbeeld: Stel $a = 23$, $m = 5$ en $n = 8$.

- We berekenen het rechterlid: $23^5 = 6436343$ zodat $6436343 \pmod 8 = 7$ (want $6436343 = 804542 \times 8 + 7$)
- We berekenen het linkerlid:
  - $a \pmod n = 23 \pmod 8 = 7$
  - $7^5 = 16807$
  - $16807 \pmod 8 = 7$ (want $16807 = 2100 \times 8 + 7$)

Toepassing bankrekeningen - Nederland

Een rekeningnummer bestaat uit 9 cijfers:

$$c_9c_8c_7c_6c_5c_4c_3c_2c_1$$

Een rekeningnummer is **geldig** wanneer:

$$9 \times c_9 + 8 \times c_8 + 7 \times c_7 + \cdots + 2 \times c_2 + c_1 \equiv 0 \pmod{11}.$$

M.a.w. de som die berekend wordt moet steeds een veelvoud zijn van 11.

Toepassing bankrekeningen - Nederland

$$45824365c_1$$

bepaal

$$\begin{aligned}
&9 \times 4 + 8 \times 5 + 7 \times 8 + 6 \times 2 + 5 \times 4 + 4 \times 3 + 3 \times 6 + 2 \times 5 \\
&= 36 + 40 + 56 + 12 + 20 + 12 + 18 + 10 \\
&= 3 + 7 + 1 + 1 + 9 + 1 + 7 + 10 \\
&= 6
\end{aligned}$$

Om een veelvoud van 11 te bekomen moet $c_1 = 5$.

Toepassing bankrekeningen

Beschouw het volgende “rekeningnummer”:

$$734160221$$

Verifieer of dit een geldig rekeningnummer is.

RSA

Inverse modulo n

We zeggen dat a en b elkaars **inverse** zijn modulo n wanneer geldt dat:

$$a \times b \pmod{n} = 1.$$

Voorbeeld: 3 en 5 zijn elkaar inverse modulo 7 want:

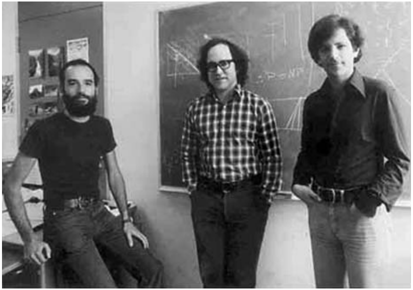
$$3 \times 5 = 15 = 2 \times 7 + 1,$$

m.a.w.

$$3 \times 5 \pmod{7} = 1.$$

RSA: een voorbeeld van asymmetrische encryptie

- Bedacht door **R**ivest–**S**hamir–**A**dleman in 1978.
- Eén van de eerste asymmetrische encryptiesystemen.
- Gebruikt modulo rekenen.



RSA algoritme

Alice wil een boodschap zenden naar Bob.
Enkel Bob mag in staat zijn om de ciphertext terug om te zetten naar de plaintext.
De volgende stappen zijn nodig:

- Bob genereert een publieke en private sleutel.
- Bob geeft de publieke sleutel aan Alice.
- Alice encrypteert de boodschap met de publieke sleutel van Bob.
- Bob gebruikt zijn private sleutel om de boodschap te decrypteren.

Opmerking: Eve beschikt *niet* over de private sleutel en kan de ciphertext m.a.w. niet ontcijferen.

RSA Algoritme : Sleutelgeneratie

- Bob kiest 2 grote priemgetallen (100 cijfers of meer). Laten we die getallen p en q noemen.
- Bob berekent $n = pq$.
- Bob berekent $\varphi(n) = (p-1)(q-1)$. Bob kiest een getal e dat geen factoren gemeenschappelijk heeft met $\varphi(n)$.
- Bob bepaalt de inverse modulo van e module $\varphi(n)$. Dit getal noemen we d.

Bob's **publieke sleutel** is (n, e).

Bob's **private sleutel** is d. Deze private sleutel moet **geheim** blijven.

Priemgetallen?

Priemgetallen zijn de bouwstenen van alle andere getallen: elk getal kan op een unieke manier gefactoriseerd worden in priemgetallen.

Bv.

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

Er zijn **oneindig veel** priemgetallen.

Wat is $\varphi(n)$?

$\varphi(n)$ telt het aantal getallen tussen 1 en $n-1$ die geen priemfactoren gemeenschappelijk hebben met n; m.a.w. het aantal getallen a tussen 1 en $n-1$ waarvoor $\gcd(a,n)=1$.

Beschouw $n = 15$. Merk op dat $15 = 3 \times 5$.
Wat zijn de getallen die wél priemfactoren gemeenschappelijk hebben met 15?

$$3, 6, 9, 12, 5, 10$$

Dus 4 veelvouden van 3 en 2 veelvouden van 5:

$$15 - 1 - 4 - 2 = 8.$$

In het algemeen: als $n = pq$:

$$\varphi(n) = pq - 1 - (p-1) - (q-1) = (p-1)(q-1).$$

RSA Algoritme : Sleutelgeneratie

- Stel dat $p = 11$ en $q = 13$ worden gekozen.
- $n = 11 \times 13 = 143$.
- $\varphi(n) = 10 \times 12 = 120$.
- Stel dat $e = 7$ wordt gekozen. (Dit is OK want $\gcd(120, 7) = 1$.
- We moeten de inverse van e vinden modulo 120.)
  Met het **uitgebreide algoritme van Euclides** vinden we dat $d = 103$.
  Inderdaad $7 \times 103 = 721 = 6 \times 120 + 1$, en dus is $7 \times 103 \pmod{120} = 1$.

RSA Algoritme: Encryptie

- Alice wil een boodschap (plaintext) m verzenden naar Bob. Alice gebruikt hiertoe de **publieke** sleutel (n, e) van Bob.
- Alice berekent
$$c = m^e \pmod{n}.$$
  c is de ciphertext die naar Bob wordt verstuurd.
- Merk op: de plaintext is m.a.w. een natuurlijk getal kleiner dan n.

RSA Algoritme: Encryptie

- Alice wil de boodschap (plaintext) $m = 9$ verzenden naar Bob. Alice gebruikt hiertoe de **publieke** sleutel $(n, e) = (143, 7)$ van Bob.
- Alice berekent

$$\begin{aligned} c &= m^e \pmod{n} \\ &= 9^7 \pmod{143} \\ &= 9 \times 9^3 \times 9^3 \pmod{143} \\ &= 9 \times 14 \times 14 \\ &= 1764 \pmod{143} \\ &= 48. \end{aligned}$$

c is de ciphertext die naar Bob wordt verstuurd.

RSA Algoritme: Decryptie

- Bob ontvangt de ciphertext c van Alice. Hij gebruikt zijn **private** sleutel d om deze te ontcijferen.
- Bob berekent
$$c^d \pmod{n}.$$
Dit zal steeds resulteren in de oorspronkelijke boodschap m!

RSA Algoritme: Decryptie

- Bob ontvangt de ciphertext $c = 48$ van Alice. Hij gebruikt zijn **private** sleutel $d = 103$ om deze te ontcijferen.
- Bob berekent

$$
\begin{aligned}
c^d \pmod{n} &= 48^{103} \pmod{143} \\
&= 48 \times (48^{51})^2 \pmod{143} \\
&= 48 \times (48 \times (48^{25})^2)^2 \pmod{143} \\
&= 48 \times (48 \times ((48^5)^5)^2)^2 \pmod{143} \\
&= 48 \times (48 \times (133^5)^2)^2 \pmod{143} \\
&= 48 \times (48 \times (100)^2)^2 \pmod{143} \\
&= 48 \times (48 \times 133)^2 \pmod{143} \\
&= 48 \times (92)^2 \pmod{143} \\
&= 48 \times 27 \pmod{143} \\
&= 1296 \pmod{143} \\
&= 9 \pmod{143}.
\end{aligned}
$$

Waarom werkt dit? Kleine stelling van Fermat

De **kleine stelling van Fermat** zegt dat: Voor elk priemgetal p en elk getal a dat niet deelbaar is door p geldt:

$$a^{p-1} \pmod p = 1$$

Voorbeeld $a = 5$ en $p = 7$:
$5^6 = 15625 = 1 + 15624 = 1 + 7 \times 2232$, en dus

$$5^6 \pmod 7 = 1 \pmod 7$$

Meer algemeen geldt de **stelling van Euler**: Voor elke a en n met $\gcd(a, n) = 1$ geldt

$$a^{\varphi(n)} \pmod n = 1.$$

Waarom werkt dit?

- Herinner je: de getallen e en d zijn zodanig gekozen dat $ed \pmod{\varphi(n)} = 1$, ofte er bestaat een k zodat

$$ed = 1 + k\varphi(n)$$

- $c = m^e \pmod n$, en wat Bob dus berekent bij het ontcijferen is

$$c^d = (m^e \pmod n)^d = m^{ed} \pmod n.$$

Nu geldt:

$$\begin{aligned} m^{ed} \pmod n &= m^{1+k\varphi(n)} \pmod n \\ &= m(m^{\varphi(n)})^k \pmod n \\ &= m1^k \pmod n \\ &= m. \end{aligned}$$

(Bewijs enkel geldig indien $\gcd(m, n) = 1$.)

Waarom is dit moeilijk te kraken

- RSA is zo moeilijk te ontcijferen omdat het haast niet te doen is om van een enorm getal n te vinden uit welke twee priemgetallen n is opgebouwd. Als n uit veel meer priemfactoren zou bestaan zou dat veel makkelijker te vinden zijn, want zodra je er dan eentje hebt gevonden kun je n 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 m dat je wilt versturen mag niet groter zijn dan n. Als dat wel zo is, dan moet je het eerst in kleinere stukken hakken en die één voor één doorsturen.

RSA: Samenvatting

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

Voorbeeld

Voorbeeld

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

Voorbeeld

- Als priemgetallen nemen we $p = 74471$ en $q = 98773$.
- De modulus $n = p \times q = 7355724083$. Het getal $\varphi(n) = (p-1)(q-1) = 7355550840$.

Voorbeeld

- Als priemgetallen nemen we $p = 74471$ en $q = 98773$.
- De modulus $n = p \times q = 7355724083$. Het getal $\varphi(n) = (p-1)(q-1) = 7355550840$.
- Voor e kiezen we 619. Het (uitgebreide) algoritme van Euclides leert ons dat $\gcd(e, n) = 1$ en dat de inverse d van e modulo $\varphi(n)$ gelijk is aan 4313513659.

Voorbeeld

- Als priemgetallen nemen we $p = 74471$ en $q = 98773$.
- De modulus $n = p \times q = 7355724083$. Het getal $\varphi(n) = (p-1)(q-1) = 7355550840$.
- Voor e kiezen we 619. Het (uitgebreide) algoritme van Euclides leert ons dat $\gcd(e, n) = 1$ en dat de inverse d van e modulo $\varphi(n)$ gelijk is aan 4313513659.
- Neem nu als boodschap PRIEM. In cijfers wordt dat $m = 1618090513$. Vercijferen levert:

$$c = 1618090513^{619} \pmod{7355724083} = 633613585$$

Voorbeeld

- Als priemgetallen nemen we $p = 74471$ en $q = 98773$.
- De modulus $n = p \times q = 7355724083$. Het getal $\varphi(n) = (p-1)(q-1) = 7355550840$.
- Voor e kiezen we 619. Het (uitgebreide) algoritme van Euclides leert ons dat $\gcd(e, n) = 1$ en dat de inverse d van e modulo $\varphi(n)$ gelijk is aan 4313513659.
- Neem nu als boodschap PRIEM. In cijfers wordt dat $m = 1618090513$. Vercijferen levert:

$$c = 1618090513^{619} \pmod{7355724083} = 633613585$$

- Ontcijferen levert.

$$c^d \pmod{7355724083} = 1618090513$$

Voorbeeld

- Als priemgetallen nemen we $p = 74471$ en $q = 98773$.
- De modulus $n = p \times q = 7355724083$. Het getal $\varphi(n) = (p-1)(q-1) = 7355550840$.
- Voor e kiezen we 619. Het (uitgebreide) algoritme van Euclides leert ons dat $\gcd(e, n) = 1$ en dat de inverse d van e modulo $\varphi(n)$ gelijk is aan 4313513659.
- Neem nu als boodschap PRIEM. In cijfers wordt dat $m = 1618090513$. Vercijferen levert:

$$c = 1618090513^{619} \pmod{7355724083} = 633613585$$

- Ontcijferen levert.

$$c^d \pmod{7355724083} = 1618090513$$

- We zien dat we inderdaad de originele boodschap terugvinden.

Ontcijferen met verkeerde sleutel

- Stel dat we de boodschap proberen te ontcijferen met een willekeurige d, bv. $d = 12345678$.
- We vinden dan

$$c^{12345678} \pmod{7355724083} = 1523535615$$

- We zien dat we een volledig andere boodschap krijgen!

Wie is de verzender?

- Alice kan nu een boodschap verzenden naar Bob die enkel door Bob kan gelezen worden.
- Hoe kan Bob weten dat de boodschap van Alice afkomstig is en niet van Eve?

Wie is de verzender?

- Alice kan nu een boodschap verzenden naar Bob die enkel door Bob kan gelezen worden.
- Hoe kan Bob weten dat de boodschap van Alice afkomstig is en niet van Eve?
- Antwoord: dat is op dit moment *niet* mogelijk. Iedereen kan een boodschap sturen naar Bob.

Wie is de verzender?

- Hoe bewijst men in het “echte” leven wie de verzender is van een bepaalde boodschap/brief?

Wie is de verzender?

- Hoe bewijst men in het “echte” leven wie de verzender is van een bepaalde boodschap/brief?
- Men plaatst een handtekening.

Wie is de verzender?

- Hoe bewijst men in het “echte” leven wie de verzender is van een bepaalde boodschap/brief?
- Men plaatst een handtekening.
- De assumptie is dat enkel de “echte” persoon in staat is de handtekening te plaatsen.

Wie is de verzender?

- Hoe bewijst men in het “echte” leven wie de verzender is van een bepaalde boodschap/brief?
- Men plaatst een handtekening.
- De assumptie is dat enkel de “echte” persoon in staat is de handtekening te plaatsen.
- Alice moet m.a.w. iets doen wat door niemand anders kan gedaan worden.

Wie is de verzender?

- Alice genereert een private d_A en een publieke sleutel (n_A, e_A).

Wie is de verzender?

- Alice genereert een private d_A en een publieke sleutel (n_A, e_A).
- Alice bezorgt de **publieke** sleutel aan Bob. (Op zo'n manier dat Bob zeker is dat de sleutel van Alice is.)

Wie is de verzender?

- Alice genereert een private d_A en een publieke sleutel (n_A, e_A).
- Alice bezorgt de **publieke** sleutel aan Bob. (Op zo'n manier dat Bob zeker is dat de sleutel van Alice is.)
- Wanneer Alice de boodschap m naar Bob wil zenden dan ondertekent ze de boodschap met haar private sleutel:

$$m_1 = m^{d_A} \pmod{n_A}.$$

Wie is de verzender?

- Alice genereert een private d_A en een publieke sleutel (n_A, e_A).
- Alice bezorgt de **publieke** sleutel aan Bob. (Op zo'n manier dat Bob zeker is dat de sleutel van Alice is.)
- Wanneer Alice de boodschap m naar Bob wil zenden dan ondertekent ze de boodschap met haar private sleutel:

$$m_1 = m^{d_A} \pmod{n_A}.$$

- Wanneer Bob de boodscahp m_1 ontvangt, dan kan hij **verifiëren** dat de boodschap van Alice afkomstig is door

$$m_1^{e_A} \pmod{n_A}$$

te berekenen.

Probleem ?

Probleem ?

Iedereen kan de boodschap m_1 zien en iedereen met de publieke sleutel van Alice kan de boodschap lezen!

Probleem ?

Iedereen kan de boodschap m_1 zien en iedereen met de publieke sleutel van Alice kan de boodschap lezen!

Oplossing: pas encryptie toe op de getekende boodschap.

- Alice wil m verzenden naar Bob:
- Alice berekent $m_1 = m_A^d \pmod{n_A}$.
- Alice berekent vervolgens $c = m_1^{e_B} \pmod{n_B}$.
- Wanneer Bob de boodschap ontvangt dan gebruikt hij zijn private sleutel om m_1 te berekenen:

$$m_1 = c^{d_B} \pmod{n_B}$$

- Vervolgens gebruikt hij de publieke sleutel van Alice om de handtekening te verifiëren:

$$m = m_1^{e_A} \pmod{n_A}.$$

Zend elkaar een getekende en vercijferde boodschap

Gebruik de Python-code om elkaar een getekende én vercijferde boodschap te verzenden.