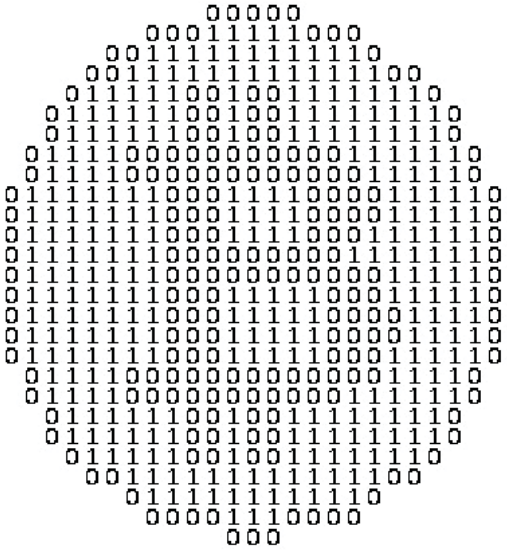
Cryptografie: de wetenschap van geheimen



Benne de Weger
b.m.m.d.weger@tue.nl

augustus 2018

TU/e Technische Universiteit Eindhoven University of Technology

Where innovation starts

Cryptografie als Informatiebeveiliging

beveiliging: doe iets tegen risico's

informatie-risico's en eisen:

- informatie komt in verkeerde handen – vertrouwelijkheid
- informatie is incorrect – integriteit
- informatie komt uit een verkeerde bron – authenticiteit
- informatie is er niet – beschikbaarheid

cryptografie helpt met de eerste drie

- traditioneel: versleuteling
- modern: ook hashing, digitale handtekeningen

communicatiemodel

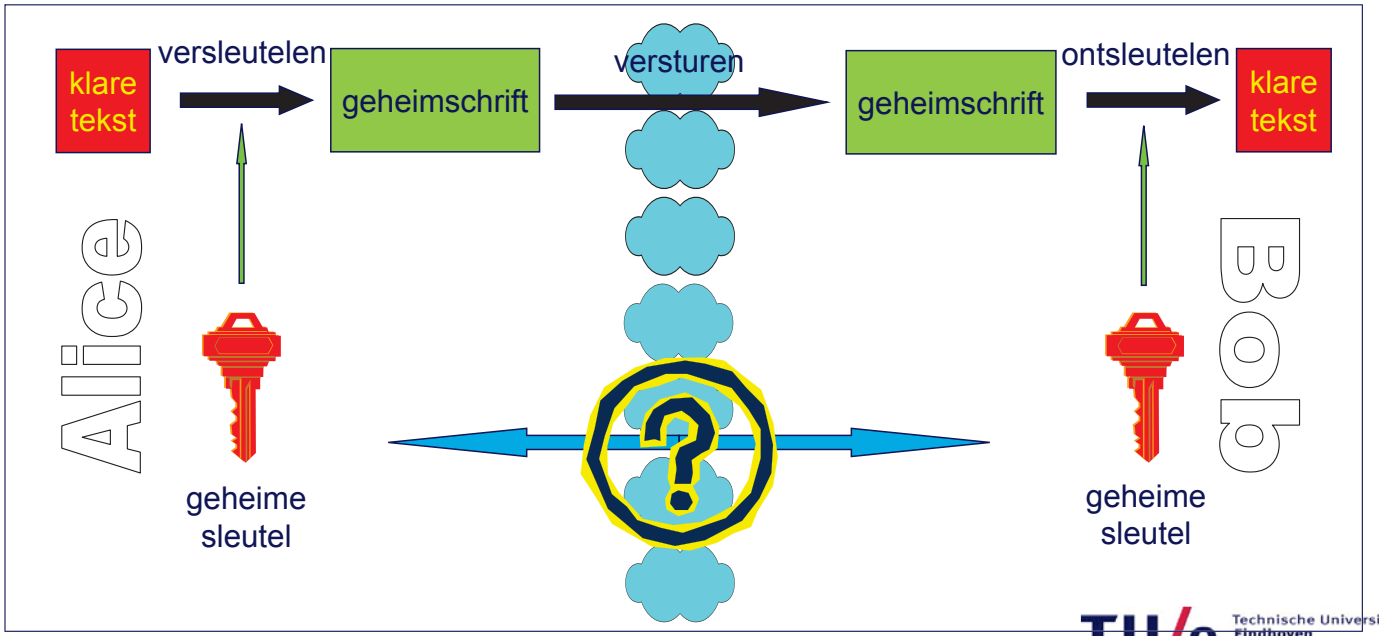
wat betekent “veilig”?

- **vertrouwelijk: Eva kan de berichten *niet lezen***
- **integer: Eva kan de berichten *niet veranderen***
- **authentiek: Eva kan zich *niet als Alice voordoen***

andere doelen

- **anonimiteit, onloochenbaarheid, onontkenbaarheid, transparantie, privacy, …**

symmetrische versleuteling



Caesar-method, substitutiemethode

Caesar-versleuteling: rotatie in het alphabet

- sleutel: aantal posities van verschuiving naar rechts
- originele Caesar-methode: sleutel = 3

  A→D, B→E, …, V→Y, W→Z, X→A, Y→B, Z→C

substitutie-method: random vaste permutatie

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓
MNBVCXZLKJHGFDSAPOIUYTREWQ
```

hoeveel sleutels?

hoe te kraken?

blokversleuteling

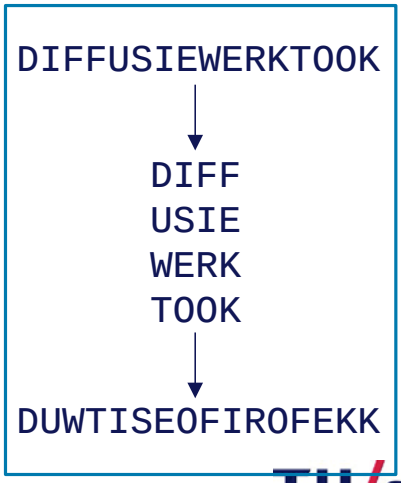
versleutelt bericht van vaste lengte (letters of bits)

- Caesar: 1 letter
- padding is nodig: voeg loze bits toe om veelvoud van bloklengte te krijgen

- voordeel: ontwerp voor vaste lengte
- plak versleutelde blokken aan elkaar

ontwerpprincipes

- confusie (substitutie, Caesar)
- diffusie (transpositie)



symmetrische algoritmen

prehistorisch (t/m begin 20e eeuw)

- Caesar, Vigenère

historisch (tot jaren 60)

- versleutelmachines: Enigma, Hagelin

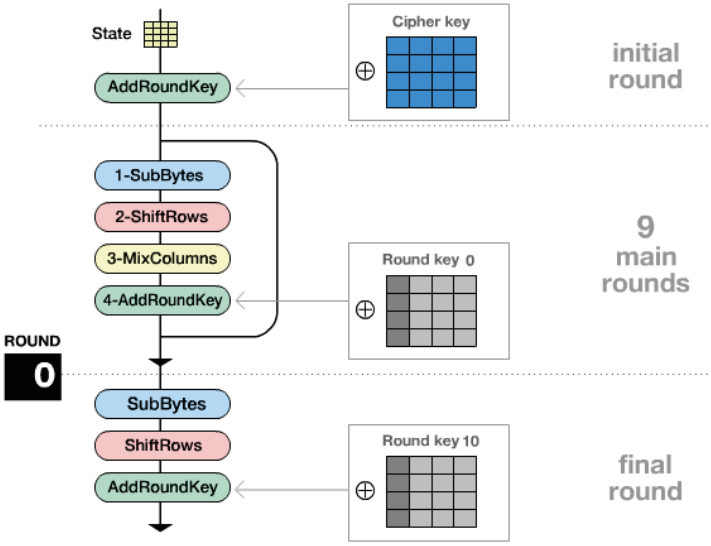
modern (vanaf jaren 70)

- blokcijfers: DES, IDEA, Blowfish, AES, Kasumi, ...
- stroomcijfers: RC4, AS/1, Salsa20, ...

AES – Rijndael

- werkt op 128-bits blokken
- sleutels van 128, 192 of 256 bits
- snel in hardware en software

- NIST standaard sinds 2002
  - winnaar van open competitie
  - ontwerpers:
    - Vincent Rijmen (nu KU Leuven)
    - Joan Daemen (nu Radboud Uni)



symmetrische cryptanalyse

aanval met brute kracht

- ontsleutel met alle mogelijke sleutels

AES met 128 bit sleutels: geen betere aanval bekend

- aantal mogelijke sleutels: $2^{128} \approx 3.4 \times 10^{38}$
- een goed algoritme met *k* bits sleutels
  heeft cryptanalytische complexiteit van 2^k ontsleuteloperaties

de kracht van machten

berekening van 2^{64} (16E) eenvoudige operaties is realistisch

- maar probeer dit niet thuis
- kraken van 64 bits sleutel met 64 processoren
  lukt misschien in een jaar
- er zijn 2 miljard computers op de wereld
- 2^{128} = 600 miljoen millennia
- dan heb je 1 bericht gekraakt

1	2	4	8	16	32	64	128	256	512	
1K	2K	4K	8K	16K	32K	64K	128K	256K	512K	Kilo
1M	2M	4M	8M	16M	32M	64M	128M	256M	512M	Mega
1G	2G	4G	8G	16G	32G	64G	128G	256G	512G	Giga
1T	2T	4T	8T	16T	32T	64T	128T	256T	512T	Tera
1P	2P	4P	8P	16P	32P	64P	128P	256P	512P	Peta
1E	2E	4E	8E	16E	32E	64E	128E	256E	512E	Exa
1Z	2Z	4Z	8Z	16Z	32Z	64Z	128Z	256Z	512Z	Zetta
1Y	2Y	4Y	8Y	16Y	32Y	64Y	128Y	256Y	512Y	Yotta
2^{90}	2^{91}	2^{92}	2^{93}	2^{94}	2^{95}	2^{96}	2^{97}	2^{98}	2^{99}	
2^{100}	2^{101}	2^{102}	2^{103}	2^{104}	2^{105}	2^{106}	2^{107}	2^{108}	2^{109}	
2^{110}	2^{111}	2^{112}	2^{113}	2^{114}	2^{115}	2^{116}	2^{117}	2^{118}	2^{119}	
2^{120}	2^{121}	2^{122}	2^{123}	2^{124}	2^{125}	2^{126}	2^{127}	2^{128}		

De Wet van Moore

snelheid van nieuwste processor verdubbelt elke 18 maanden

- geldt vanaf 1960, en nog steeds (experimenteel)
- cryptografisch gevolg: de kosten van een brute kracht-aanval halveren elke 18 maanden

voor goed symmetrisch algoritme: met 1 bit langere sleutel

- verdubbelt het aantal mogelijke sleutels
- verdubbelt de hoeveelheid werk voor de aanvaller
- versleutelen en ontsleutelen wordt maar een klein beetje langzamer

De Wet van Moore werkt dus in het voordeel van de cryptografen en in het nadeel van de aanvallers

asymmetrische versleuteling

geldkistje: metafoor voor symmetrische versleuteling

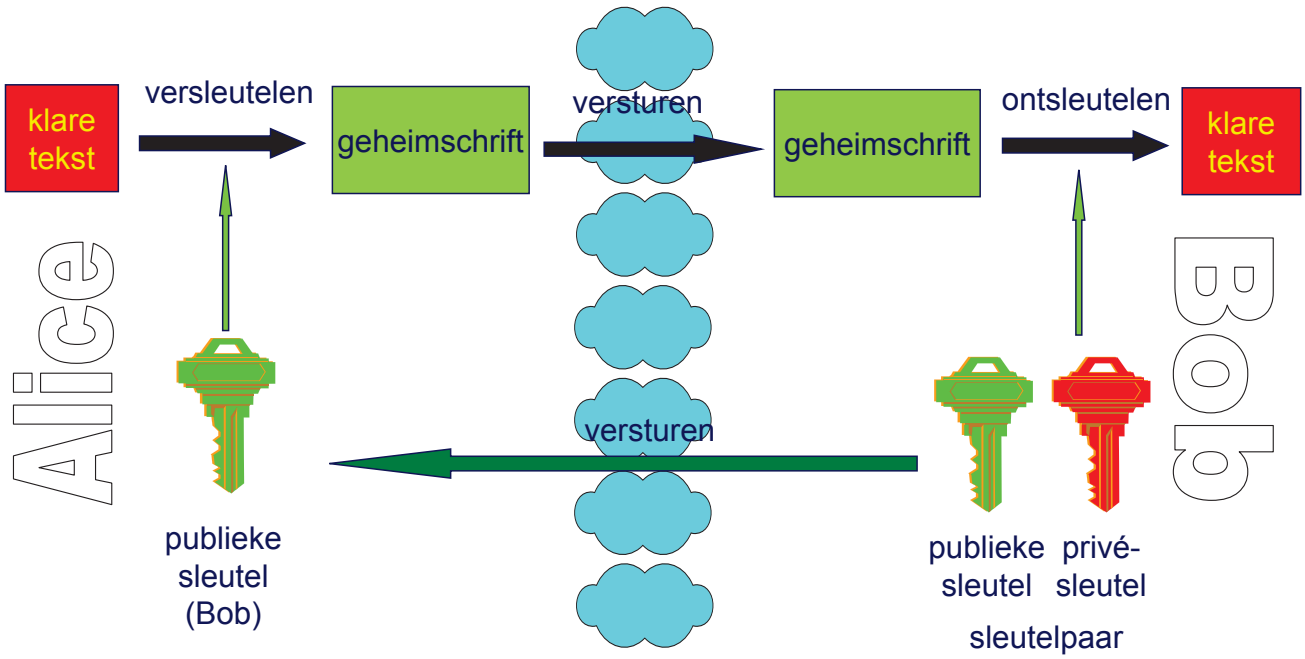
- probleem: hoe krijgen Alice en Bob dezelfe sleutel

asymmetrische versleuteling: denk aan een hangslot

- hangslot kan gesloten worden zonder het sleuteltje

kunnen we dit gebruiken in de digitale cryptografie?

asymmetrische versleuteling



asymmetrische versleuteling

- **voorbeelden**
  - **RSA (Rivest, Shamir, Adleman) 1977**
  - **Diffie-Hellman / ElGamal, Elliptische Krommen-varianten, NTRU, ...**
- **doorgaans gebaseerd op getaltheorie**
  - **de publieke sleutel bevat informatie over de privé-sleutel maar dat mag niet uitlekken**
- **veiligheid gebaseerd op *moeilijke problemen* zoals**
  - **ontbinden in priemfactoren (RSA)**
  - **discrete logaritmen (Diffie-Hellman, ElGamal)**
    - **Elliptische Krommen-variant**
  - **roosterproblemen (NTRU)**

asymmetrische cryptanalyse

- asymmetrische cryptografie gebaseerd op getaltheorie
  - er is een hoop structuur
  - kraakmethoden vaak beter dan brute kracht
  - daarom vaak langere sleutels (vergeleken met symmetrische crypto)
- moeilijkheid van ontbinden in priemfactoren
  - hooguit sub-exponentieel:

    k bits RSA-modulus → breektijd is $\exp(2k^{1/3})$

    huidige record (sinds 2010): 768 bits
- waarom is ontbinden in factoren moeilijk?

  dat weten we niet echt…

de veiligheid van cryptografie berust op de domheid van de wiskundigen

sleutellengtes: symmetric vs. asymmetric

- model van Lenstra en Verheul voor civiele toepassingen
  - zie www.keylength.com
  - schat je tegenstander in
  - bedenk tot wanneer je je informatie beschermd wilt hebben

met cryptografie koop je alleen tijd

jaar	symm.	asymmetrisch (factoriseren, discr. logs)		asymm. (ellipt. kr)
		optimistisch	conservatief	
2025	85	1538	1805	170
2026	86	1569	1855	171
2027	86	1601	1906	172
2028	87	1633	1958	174
2029	88	1665	2010	175

- vandaag algemeen geaccepteerd als voorlopig voldoende:
  - symmetrisch: minstens 128
  - asymmetrisch: RSA minstens 2048

    ECC: minstens 256

modulorekenen

klokrekenen op een klok met m uren
- m = 12, 24, 17, 23783905905230589057589957, ...
- m heet *modulus*

$a \equiv b \pmod{m}$ betekent: a en b verschillen een m-voud
- optellen, aftrekken, vermenigvuldigen kan altijd
- altijd terugrekenen naar een getal in $\{0,1,2,...,m\text{-}1\}$
  (delen met rest door m, houd alleen de rest)

delen kan fout gaan: $21 \equiv 6 \pmod{15}$ maar $7 \not\equiv 2 \pmod{15}$

machtsverheffen:
- wel: als $a \equiv b \pmod{m}$ dan $a^n \equiv b^n \pmod{m}$
- maar let op: modulus niet toepassen in de exponent:
- $10 \equiv 3 \pmod{7}$ maar $2^{10} \equiv 2 \pmod{7}$, terwijl $2^3 \equiv 1 \pmod{7}$

stelling van Fermat

als modulus een priemgetal p is, dan geldt voor elke a = 1, 2, ..., p-1

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

als modulus een priemgetal p is, dan kun je dus *wel* delen:

$$a^{p-2} \equiv \text{"}1/a\text{"} \pmod{p}$$

met exponenten rekenen doe je niet (mod p) maar (mod p-1)

$2^{10} \equiv 2 \pmod{7}$, dus $2^4 \equiv 2 \pmod{7}$ want $10 \equiv 4 \pmod{7\text{-}1}$

$F_p = \{0, 1, 2, ..., p\text{-}1\}$ is een *additieve* groep

$F_p^* = \{1, 2, ..., p\text{-}1\}$ is een *multiplicatieve* groep

F_p^* is zelfs *cyclisch*: er is altijd een *voortbrenger* g zodat

$$F_p^* = \{1=g^0, g=g^1, g^2, g^3, ..., g^{p-2}\}$$

voorbeeld: p = 19, g = 2

machtsverheffen

machtsverheffen (mod p) gooit de boel flink door elkaar:

telkens verdubbelen (mod 19) geeft machten van 2:

- **1, 2, 4, 8, 16, 32 ≡ 13, 26 ≡ 7, 14, 28 ≡ 9, 18, 36 ≡ 17, 34 ≡ 15, 30 ≡ 11, 22 ≡ 3, 6, 12, 24 ≡ 5, 10, 20 ≡ 1 (mod 19)**

snel machtsverheffen: gebruik *kwadrateer-en-vermenigvuldig*-methode:

- **$23 = 2^4 + 2^2 + 2^1 + 2^0$ (binaire schrijfwijze)**
- **dus $a^{23} = a^{16} \cdot a^4 \cdot a^2 \cdot a$ kost 3 vermenigvuldigingen na 4 kwadrateringen:**

$$a \to a^2 \to a^4 \to a^8 \to a^{16}$$

- **a^n kost maximaal $\log_2 n$ vermenigvuldigingen na $\log_2 n$ kwadrateringen**

orde van een getal a: de kleinste positieve n zodat $a^n \equiv 1 \pmod p$

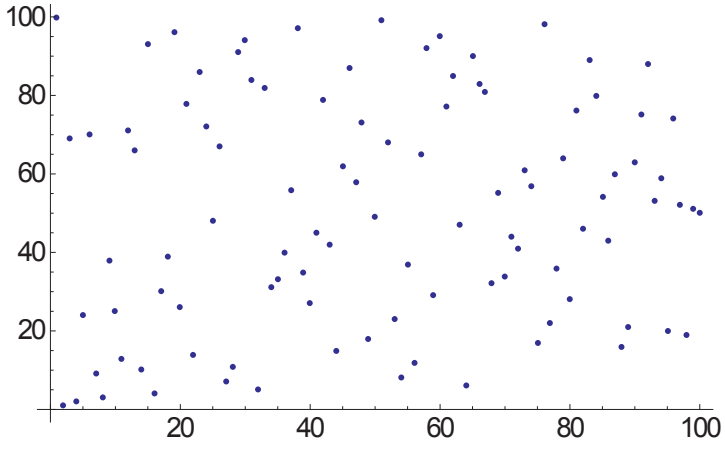
orde van 2 modulo 19 is 18

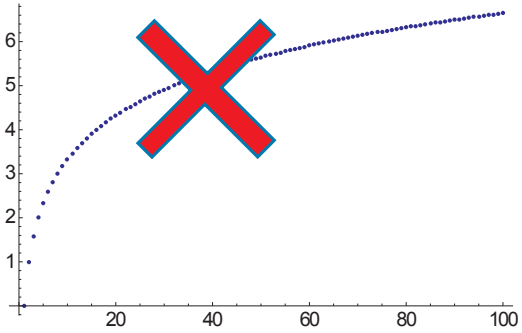
orde van 11 modulo 19 is 3

Discrete Logaritme

discrete logaritme: gegeven p, g en y zodat $y \equiv g^x \pmod p$, vind x

- **dit is een even moeilijk probleem als ontbinden in factoren!**





Diffie-Hellman sleuteluitwisseling

Diffie-Hellman systeemparameters

- modulus: een groot priemgetal p
- voortbrenger: g met $1 < g < p - 1$

Diffie-Hellman sleutelpaar

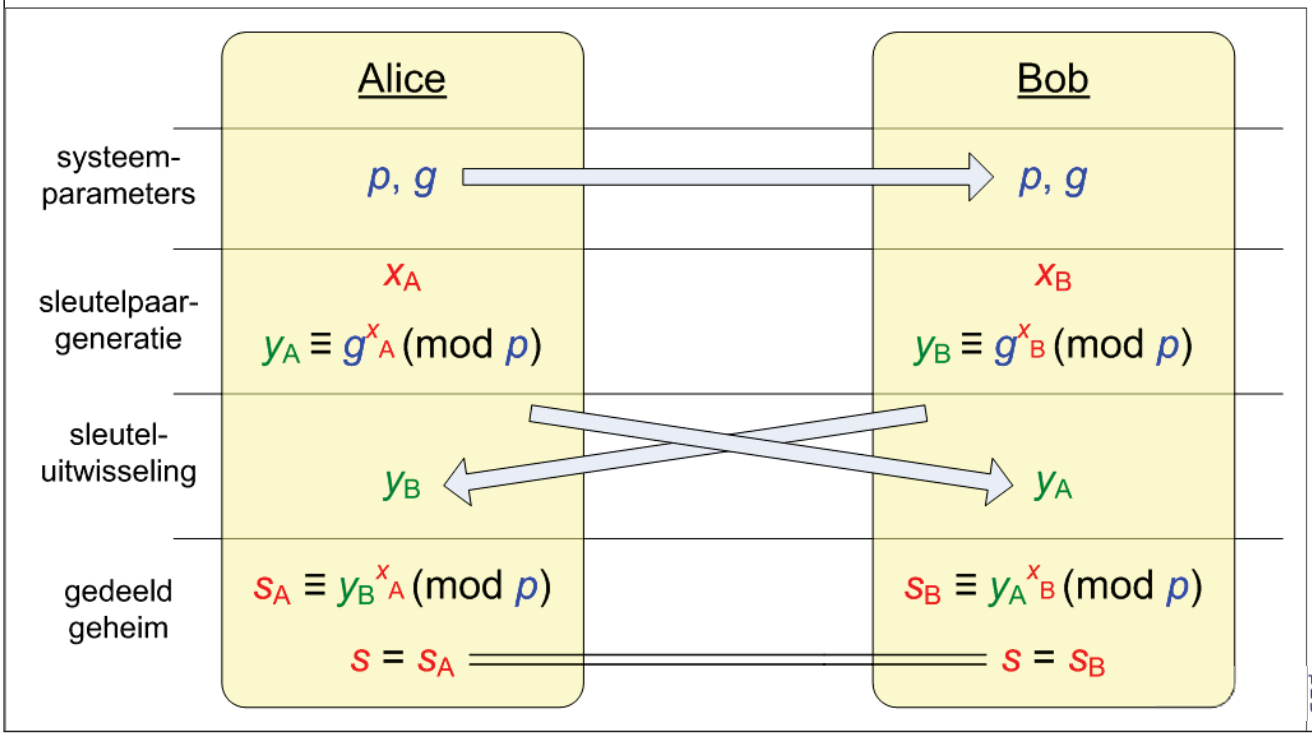
- privé-sleutel: random geheel getal x met $1 < x < p - 1$
- publieke sleutel: $y \equiv g^x \pmod{p}$

voorbeeld:
(met kleine getallen)
$p = 19$, $g = 3$

$x = 5$, $y = 15$
omdat $3^5 = 243 \equiv 15 \pmod{19}$

$x = 6$, $y = 7$
omdat $3^6 = 729 \equiv 7 \pmod{19}$

Diffie-Hellman sleuteluitwisseling



Diffie-Hellman sleuteluitwisseling

systeemparameters: $p = 19$, $g = 3$

sleutelpaar van Alice: $x_A = 5$, $y_A = 15$

sleutelpaar van Bob: $x_B = 6$, $y_B = 7$

Alice berekent: $s_A = 7^5 \equiv 11 \pmod{19}$

Bob berekent: $s_B = 15^6 \equiv 11 \pmod{19}$

het gedeelde geheime getal is nu $s = 11$

ElGamal-versleuteling

Bob heeft een permanent sleutelpaar:

- privé-sleutel x_B, publieke sleutel $y_B \equiv g^{x_B} \pmod{p}$

Alice maakt een eenmalig sleutelpaar:

- privé-sleutel x_1, publieke sleutel $y_1 \equiv g^{x_1} \pmod{p}$

hiermee maken ze een eenmalig gedeeld Diffie-Hellman geheim s

Alice versleutelt m: simpelweg vermenigvuldigen (mod p):

$$c \equiv m\, s \pmod{p}$$

Bob ontsleutelt c : simpelweg delen (mod p):

$$m \equiv c/s \pmod{p}$$

RSA versleutelen

Bob maakt sleutelpaar:

- modulus $n = p\,q$, p en q zijn grote priemgetallen
- hulpgetal $\varphi = (p-1)\,(q-1)$
- publieke exponent e (willekeurig tussen 3 en φ)
  - zodat e en φ geen delers gemeen hebben
- privé-exponent d zodat $e\,d \equiv 1 \pmod{\varphi}$

publieke sleutel: n, e, privé-sleutel: (n,) d

Alice versleutelt bericht m door machtsverheffing modulo n:

$$c \equiv m^e \pmod{n}$$

Bob onsleutelt c: ook door machtsverheffing (mod n):

$$m \equiv c^d \pmod{n}$$

waarom werkt RSA?

Bob berekent

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

bedenk: p is een deler van n dus

$$c^d \equiv m^{ed} \pmod{p}$$

Fermat: neem $ed \pmod{p-1}$

maar verband tussen e en d was: $ed \equiv 1 \pmod{p-1}$

dus $c^d \equiv m^1 = m \pmod{p}$ dus $c^d - m$ is een p-voud

voor q net zo: $c^d - m$ is ook een q-voud

dus is het een n-voud, dus is $c^d \equiv m \pmod{n}$