MATH

Hoofdstuk 2: symmetrische cryptosystemen

* 2 standaartechnieken:
  + ~~Transpositie: het verwisselen van de letters van het bericht op een vooraf afgesproken manier~~
  + Substitutie: de letters vervangen door andere letters op een vooraf afgesproken manier

1. De ceasarrotatie
   1. Methode

Voorbeeld: de letter “m” wordt verzonden en de sleutel k=20

Coderen:

* Stap 1: m correspondeert met de waarde 12
* Stap 2: 12 + k = 12 + 30 = 32
* Stap 3: 32 >= 26 => 32(mod26) = 6 (immers 32/26 = 1 rest 6)
* Stap 4: hiermee correspondeert met de letter g.

Decoderen:

* Stap 1: g correspondeert met de waarde 6
* Stap 2: 6-20(k) = -14
* Stap 3: -14<0 => -14(mod 26) = -14 + 26 = 12
* Stap 4: hiermee correspondeert de letter m

1. Substitutiemethode mbv de bitoperator XOR

Coderen:

* Stap 1: aan elk karakter uit de boodschap een getalwaarde toekennen bv. De ascii-code
* Stap 2: XOR-operator gebruiken in combinatie met de gekozen sleutel.

Voorbeeld: we kiezen als sleutel het karakter R. de boodschap is de letter a. Wat krijgt de ontvanger?

ANSI (ASCII)

Coderen hexadecimaal Binair

Boodschap a 6 1 0110 0001  
Sleutel R 52 0101 0010

Gecodeerde  
boodschap 0011 0011

De ontvanger krijgt het getal 3 toegestuurd

Decoderen:

* Stap 1: aan elk karakter uit de boodschap een getalwaarde toekennen op dezelfde manier als gebeurd is bij het coderen.
* Stap 2: XOR-operator gebruiken in combinatie met de gekozen sleutel.

Voorbeeld: de ontvanger boodschap is het getal 3, de sleutel is het karakter R. Welk karakter is er verstuurd?

decoderen hexadecimaal Binair

Boodschap 3 3 3 0011 0011  
Sleutel R 5 2 0101 0010

Gedecodeerde  
boodschap 0011 0011

Het verzonden karakter is a.

1. Blokcijfersystemen

Voorbeeld:

**Coderen:** boodschap INFORMATICA, sleutel: TIN

I N F O R M A T I C A

T I N T I N T I N T I

Omzetten naar de bijhorende numerieke waarde

8 13 5 14 17 12 0 19 8 2 0

19 8 13 19 8 13 19 8 13 19 8

Optellen

27 21 18 33 25 25 19 27 21 21 8

Modulo 26 rekenen

1 21 18 7 25 25 19 1 21 21 8

Omzetten naar tekst geeft

B V S H Z Z T B V V I

**Decoderen**

B V S H Z Z T B V V I

T I N T I N T I N T I

Omzetten naar de bijhorden numerieke waarde

1 21 18 7 25 25 19 1 21 21 8

19 8 13 19 8 13 19 8 13 19 8

Aftrekken

-18 13 5 12 17 12 0 -7 8 2 0

Zorgen dat de uitkomst >=0 is door modulo 26 te bereken

8 13 5 14 17 12 0 19 8 2 0

Omzetten naar tekst geeft

I N F O R M A T I C A

3.2 Blokcijfersystemen op basis van XOR-methode

ANSI (ASCII)

Coderen hexadecimaal Binair

Boodschap een 6 5 6 5 6 E 0110 0101 0110 0101 0110 1110  
Sleutel Tin 5 4 6 9 6 E 0101 0100 0110 1001 0110 1110

Gecodeerde  
boodschap 0011 0001 0000 1100 0000 0000

ANSI (ASCII)

Decoderen hexadecimaal Binair

Boodschap 3 1 0 C 0 0 0011 0001 0000 1100 0000 0000  
Sleutel Tin 5 4 6 9 6 E 0101 0100 0110 1001 0110 1110

Gedecodeerde  
boodschap 0110 0101 0110 0101 0110 1110

1. Enkele nadelen symmetrische cyptrosystemen

Zender en ontvanger moeten een sleutel afspreken. Hoe kan je op een beveiligde manier deze sleutel verzenden?

In een netwerk zal je veel meer sleutels moeten creëren dan er mensen op het netwerk zijn.

Vraag: a) Hoeveel sleutels heb je nodig in een netwerk van 5 personen? 10  
 b) Hoeveel sleutels heb je nodig in een netwerk van 50 personen?

N . (N -1) /2 => 50 . (50 -1) / 2 = 1225

Hoofdstuk 4: asymetrische cyptrosystemen

Uitgewerkt voorbeeld RSA

An stuurt een boodschap naar Piet.

**Coderen**

* An zet de boodschap wiskunde is leuk in ascii-code. Dit geeft

119  105  115  107 117 110  100  101 32  105  115 32  108 101 117 107

* Hoe kan An dit bericht vercijferen? Daarvoor heeft zij de openbare sleutel van piet nodig deze bestaat uit 2 getallen e = 989 en m=1073
* An kan de boodschap vercijferen door op elk karakter de volgende bewerking uit te voeren: Me (mod m) = M989(mod1073) = 282

De eerste letter geeft 119989 (mod 1073) = 282

* Wanneer An dit op elk getal toepast, bekomt An het volgende

282 549 28 342 117 36 121 1047 311 549 28 311 826 1047 117 342

**Decoderen**

* Piet ontvangt volgende boodschap van An
* 282 549 28 342 117 36 121 1047 311 549 28 311 826 1047 117 342
* Zijn privé sleutel bestaat uit 2 getallen d=53 en m=1073.
* Piet kan de geheime boodschap ontcijferen door op elk karakter de volgende bewerking uit te voeren: S(M)d (mod m) = S(M)53(mod1073)

De eerste letter geeft 28253 (mod 1073) = 119

* Wanneer Piet dit op elk getal toepast, bekomt Piet het volgende

119  105  115  107 117 110  100  101 32  105  115 32  108 101 117 107

* Dit stellen de ASCII-codes voor van de boodschap: Wiskunde is leuk

Voorbeeld: neem P=13 en q=17 => m = p . q = 221

Wanneer nu

* M=123 dan blijkt M = M13 = M25 = … modulo 221
* M=21 dan blijkt M = M5 = M9 = … modulo 221
* M=91 dan blijkt M = M17 = M33 = … modulo 221

In het bijzonder is dus M = MK+1 = M2K+1 = … modulo m.

Het merkwaardige is nu – en dat volgt uit stellingen van Fermat(1601-1665) en Euler(1707-1783) – dat k altijd een deler is van K = (p-1) . (q-1) zodat voor elke M geldt:

M = MK+1 = M2K+1 = M 3K+1 = …. Modulo m

**Vercijferen & handteken:**

BV. Geg volgende sleutels

|  |  |  |  |
| --- | --- | --- | --- |
|  | m | e | d |
| ELIEN | 7261 | 4253 |  |
| SANDER | 3959 | 2005 |  |

Sleutels controleren (voorwaarde 1)

Eumath:

>factor(7261)

-> 53, 137

>gcdext(53,137)

-> 1 (1 gemene deler -> dan is de sleutel correct)

(voorwaarde 2)

* P= 53 / g=137

e < K (ELIEN) K = (p – 1) . (q – 1) = 52 . 136 = 7072

* 4253 < 7072

d bereken:

.{ggd,d,j}:= gcdext( e, K)

->1

>d

->2165 = d(ELIEN)

Als d < 0 dan moet je er K bij optellen.

Eumath:

Ascii-waardes opvragen:   
>Ascii(“A”) = 65  
Karakter opvragen:  
>Char(65) = A  
Priemgetallen opvragen:  
>Primes(n) = geeft alle priemgetallen tot n

Coderen en Decoderen (e, d en m zijn van de ontvanger):

& mod ( ascii-waarde vd letter ^ e , m) = codering

& mod (codering ^ d , m) = ascii-waarde

Handtekenen en Dehandtekenen(e, d, en m zijn van de verzender):

& mod ( ascii-waarde ^ d , m ) = gehandtekende boodschap

& mod ( geh. Boodschap ^ e , m) = ascii - waarde