Inhoudsopgave

Lijst van figuren

Lijst van tabellen

Hoofdstuk 1

Inleiding

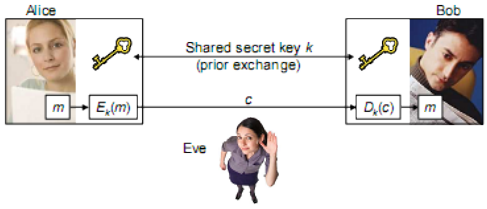
Hoofdstuk 2

Encryptie - Applicaties

Citations needed

Sinds het begin der tijden is er een nood geweest aan manieren om berichten versleuteld te verzenden tussen twee partijen. Voorbeelden van enkele klassieke encryptiemethoden zijn het Atbashcijfer [**?**] (Babylonië, 600 v. Chr.), het Caesarcijfer [**?**] (56 n. Chr.) en het dubbele transpositie cijfer [**?**] (oa. gebruikt door weerstandsgroepen in WO II). E'en eigenschap die al deze methodes met elkaar gemeen hebben, is het gebruik van een op voorhand afgesproken sleutel. Dit principe, dat ook door vele moderne encryptiemethodes (zoals bv. 3DES [**?**] en AES [**?**]) gebruikt wordt, noemt men symetrische versleuteling.

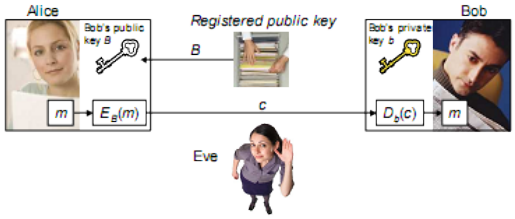
De algemene werking van zulke methodes is weergegeven in Fig. 2.1. Alice zendt een bericht m naar Bob door het te versleutelen, met een door hen beiden gekende sleutel k, die op zijn beurt met diezelfde sleutel het bericht ontcijfert. Indien Eve de vooraf afgesproken sleutel kent, kan zij uiteraard alle communicatie tussen Alice en Bob ontcijferen. Er is dus nood aan een manier om veilig een sleutel k te kunnen afspreken tussen twee partijen. Deze sleutel kan dan vervolgens bijvoorbeeld gebruikt worden in een symmetrisch sleutel algoritme.



Figuur 2.1: Algemene structuur van een symmetrische versleutelingsmethode

Een oplossing voor dit probleem was niet gekend tot en met 1976, toen Diffie en Hellman hun algoritme voor sleutel uitwisseling [**?**] publiceerden. Hun algoritme laat twee partijen toe een geheime sleutel over een onbeveiligd kanaal af te spreken. Deze ontdekking plaveide de weg voor talrijke publieke sleutel

methodes (oftewel asymmetrische sleutel methodes), waarvan de werking wordt getoond in Fig. 2.2.



Figuur 2.2: Algemene structuur van een asymmetrische versleutelingsmethode

Hoofdstuk 3

Encryptie - Wiskundige Achtergrond

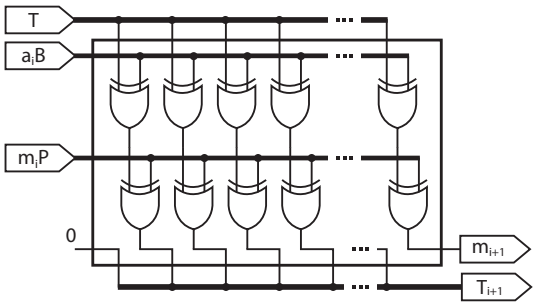
Lees alles maar in [**?**].

Hoofdstuk 4

Modular Arithmetic Logic Unit (MALU)

4.1 MALU over GF(2^m)

Blabla, MALU, hupsakee!



Figuur 4.1: Basis implementatie van een MALU-blok met $d = 1$

En nog veel meer teskt! Yes!

Hoofdstuk 5

MALU - Uitbreiding Naar Pairings

Hoofdstuk 6

MALU - Pairings - Implementatie

Hoofdstuk 7

Optimalisaties

Hoofdstuk 8

Tests

Hoofdstuk 9

Veiligheid - Side Channel Attacks

Hoofdstuk 10

Conclusie

Bijlage A

GEZEL Code