ROYAL HOLLOWAY, UNIVERSITY OF LONDON: Information Security Group - Smart Card Centre

Contra-expertise-beoordeling van de veiligheidsanalyse van de Nederlandse OV-Chipkaart door TNO[1]

Beveiligingsaspecten van de OV-Chipkaart – Korte handleiding voor niet-deskundige lezers

De huidige discussie rondom de beveiliging van de OV-Chipkaart is veroorzaakt door bepaalde ontwikkelingen van zeer technische aard en hebben te maken met specialistische gebieden zoals cryptografie, smart cards en algemene informatie over systeemveiligheid en -beveiliging. Om een beter beeld te krijgen van de problematiek, zal in dit document gepoogd worden om de meest wezenlijke punten op een eenvoudige wijze uit te leggen. De belangrijkste doelstelling is daarbij het ondersteunen van beleidsmakers bij de vorming van evenwichtige en op kennis gebaseerde zienswijzen omtrent deze aangelegenheid. Hoewel de aandacht zich zal concentreren op het Mifare Classic-algoritme, dat voor de OV-Chipkaart is gebruikt, is het van belang zich te realiseren dat dit slechts een onderdeel (hoewel een cruciaal onderdeel) vormt van de algehele systeemoplossing. De belangrijkste vraag is hoe een probleem, welk dit ook mag zijn, afbreuk doet aan de algehele veiligheid van een systeem en wie daarvan vervolgens misbruik zou proberen te maken en waarom.

Keuze van een oplossing voor systeemveiligheid en -beveiliging

Alvorens we gaan kijken naar de OV-Chipkaart is het verstandig ons eerst een situatie in te denken waarin voor twee werknemers een auto moet worden aangeschaft. Werknemer 1 bekleedt een hoge functie, is zeer belangrijk voor het bedrijf en loopt wellicht het gevaar om persoonlijk te worden aangevallen. Werknemer 2 werkt meestal achter de schermen maar werkt wel met gevoelige documenten waar dieven graag de hand op zouden willen leggen. Voor werknemer 1 zou de keuze bij de aanschaf vallen op een dure, indrukwekkende, kogelvrije limousine, terwijl werknemer 2 genoeg zou hebben aan een auto die alleen maar veilig is, betrouwbaar is in gebruik en bovendien goed kan worden afgesloten. Om voor werknemer 2 ook een limousine aan te schaffen, zou onnodige kosten met zich meebrengen.

> *Dit eenvoudige voorbeeld is bedoeld om te illustreren dat de keuze voor een beveiligingsoplossing en de daaraan verbonden kosten afhangen van hetgeen we willen beschermen (de zaken van waarde) en wat voor type bedreiging en bedreigers te verwachten zijn.* Daarbij bestaat er niet zoiets als een 100%- of 'fool-proof' beveiliging, maar moet er een kritisch evenwicht worden gevonden tussen de risico's en redelijke tegenmaatregelen – ook wel een risicomodel genoemd.

Om bij het voorbeeld van de auto's te blijven, mogen we van een nieuwe auto verwachten dat deze een redelijk aantal jaren kan worden gebruikt zonder problemen op te leveren. Daarna is hij weliswaar nog steeds bruikbaar, maar kan het zijn dat de auto iets meer op de autowerkplaats te vinden zal zijn en kunnen verbeteringen nodig zijn om waardevoller zaken te kunnen beschermen. Iemand die imagobewust is, zal de auto vervangen voordat het probleem zichtbaar wordt. Iemand die

---

[1] Dit document bevat de vertaling van het in het Engels gepubliceerde rapport *Counter Expertise Review of the TNO Security Analysis of the Dutch OV-Chipkaart*, uitgebracht door Royal Holloway University of London (RHUL) aan het Ministerie VenW. In deze vertaling is de inhoud en strekking van het oorspronkelijke rapport zo nauwkeurig mogelijk benaderd, zodat het Nederlandse parlement en publiek hiervan zonder taalbarrière kennis kunnen nemen. Om echter discussie over mogelijke interpretatie- en nuanceverschillen te voorkomen, blijft het originele Engelse eindrapport van de RHUL het enige met formele status. Hoewel aan de vertaling zowel inhoudelijk als tijdens de totstandkoming uiterste zorg is besteed, aanvaardt het ministerie geen aansprakelijkheid voor eventuele fouten en onvolkomenheden, noch voor de gevolgen hiervan.

imago niet zo belangrijk vindt, kan de auto net zolang blijven gebruiken totdat het niet meer gaat. Hiermee willen we het volgende zeggen:

> *Elke beveiligingoplossing heeft een bepaalde levenscyclus. Aan het begin van die levenscyclus moet een behoorlijk ontworpen beveiligingsoplossing vrij zijn van problemen. Als echter de technologie verouderd begint te raken, dan kan zij het doelwit worden van aanvallen. Nu kunnen deze aanvallen nog wel enige tijd onder controle worden gehouden door aanvullende maatregelen, maar uiteindelijk zal het nodig zijn om naar een verbeterde oplossing over te gaan. Zo'n overgang heet een migratie. Van invloed op zo'n besluit tot migratie zijn de kosten in vergelijking met de verliezen van de oude oplossing en ook redenen die te maken hebben met reputatie/imago.*

De OV-Chipkaart als voorbeeld van een op een smart cards gebaseerd vervoerssysteem, moet kleine en middelgrote geldbedragen beschermen tegen voornamelijk pogingen tot fraude/aanvallen door redelijk goed uitgeruste en inventieve criminelen. Van een risicomodel zou dan mogen worden verwacht dat het uitkomt bij de noodzaak voor een smart card die een gemiddeld (of hoger) veiligheidsniveau biedt en die is gebaseerd op technologie die nog steeds in een bruikbaar stadium van haar levenscyclus is.

Een beknopt overzicht van de cryptografische beveiliging van het OV-Chipkaartsysteem

Net als de meeste smart card oplossingen waarbij het gaat om transacties van een beperkte financiële waarde, is ook de smart card die wordt gebruikt voor het OV-Chipkaartsysteem uitgerust met beveiligingsmaatregelen om zowel de aanbieders van de dienst als de gebruikers ervan te beschermen. Algemene oplossingen omvatten onder meer het ontwerp van speciale beveiligingsprotocollen, dat zijn implementaties van programma's die een bepaalde beveiligingstaak vervullen, en maatregelen die het knoeien met het systeem op fysiek niveau tegengaan. In het OV-Chipkaartsysteem wordt informatie uitgewisseld tussen kaarten en kaartlezers. Het doel van deze beveiligingsmaatregelen is dan ook deze gegevensuitwisseling te beschermen en ervoor te zorgen dat het systeem zich gedraagt zoals bedoeld.

Het OV-Chipkaartsysteem maakt gebruik van de Mifare Classic-kaart, en de beveiligingsmaatregelen die in deze kaart zijn aangebracht, hebben de volgende twee belangrijkste doelstellingen:

1. De kaart moet de lezer ervan overtuigen dat de kaart authentiek is. Op zijn beurt moet de lezer de kaart ervan overtuigen dat de lezer authentiek is. Dit proces heet *wederzijdse authenticatie*. Het doel daarvan is dat zowel de lezer als de kaart overtuigd is van de authenticiteit van de andere en op grond van die overtuiging informatie begint uit te wisselen met een daartoe gerechtigde gelijkwaardige partij.
2. Het is wenselijk dat alle informatie die tussen de kaart en de lezer wordt uitgewisseld, wordt beschermd tegen onbevoegd afluisteren en onbevoegde (potentieel kwaadwillend) wijzigingen.

Dit zijn klassieke problemen bij communicatieprotocollen. Hoe die problemen moeten worden aangepakt is een van de voornaamste vraagstukken waar het vakgebied van de *cryptografie* zich mee bezighoudt. Een manier om dit te bereiken is het gebruik van cryptografische algoritmen (of "ciphers"). Dit zijn mathematische algoritmen die kunnen worden geïmplementeerd in software of hardware en complexe bewerkingen uitvoeren met gegevens. Zo kan een *versleutelingsalgoritme* worden gebruikt om gegevens te *versleutelen* (door elkaar te husselen) waardoor de oorspronkelijke boodschap onherkenbaar wordt. In het algemeen kunnen dergelijke algoritmen (en varianten daarvan) voor beveiligingsprotocollen worden gebruikt om zo de authenticiteit van alle bij het protocol betrokken partijen te bewijzen en de uitgewisselde informatie te beschermen. Het algoritme dat wordt gebruikt in de Mifare Classic-kaart heet CRYPTO1.

Echter, om dit doel te bereiken is het vereist dat de authentieke, bevoegde partijen (d.w.z. de kaart en de lezer) bepaalde geheime informatie delen die alleen zij kennen en niemand anders. Bij het OV-Chipkaartsysteem gaat het om de volgende informatie:

1. de details van het cryptografisch algoritme zelf, inclusief de structuur en de implementatie ervan;
2. een geheime reeks binaire cijfers of bits (d.w.z. 0 en 1), die door het algoritme worden gebruikt om de cryptografische bewerkingen met de tussen de lezer en de kaart uitgewisselde gegevens uit te voeren. Deze reeks wordt een *sleutel* genoemd en moet voor elke kaart uniek zijn (in feite heeft elke kaart een aantal sleutels). Een authentieke lezer kent van alle kaarten de sleutels (en kan dus met elke kaart communiceren), terwijl een kaart alleen zijn eigen sleutels kent.

We willen hierbij aantekenen dat als iemand die zou proberen het systeem aan te vallen, zowel het algoritme als een bepaalde kaartsleutel weet, deze persoon in potentie een gekloonde kaart zou kunnen maken, informatie op een authentieke kaart kan schrijven of gewoon de gegevensuitwisseling tussen een kaart en een lezer afluisteren. Er zijn een aantal scenario's waarin een aanvaller gebruik zou kunnen maken van zijn kennis van het algoritme en van de sleutel waarmee het systeem kan worden aangevallen. Meestal zijn er binnen het systeem dan ook verdere beveiligingsmaatregelen getroffen om (in elk geval) de gevolgen van zulke aanvallen te beperken. In redelijkheid kan echter

worden gesteld dat de veiligheid en beveiliging van de huidige OV-Chipkaart tot op zekere hoogte zowel afhangt van het *algoritme* als van het geheim blijven van de *sleutel*.

1 Opmerking: binnen een vervoerssysteem is sprake van meerdere lezers die het geheim van de kaart kennen.

Hier komen we echter de eerste zwakke plek voor de OV-Chipkaart tegen: de beveiliging van het systeem lijkt (in elk geval deels) afhankelijk te zijn van de geheimhouding van het cryptografische algoritme zelf. Het is binnen de cryptografie een bekend principe dat een cryptografisch systeem voor zijn beveiliging niet afhankelijk hoort te zijn van de geheimhouding van het algoritme. Dit staat bekend als het *principe van Kerckhoffs*, genoemd naar de negentiende-eeuwse Nederlandse cryptograaf Auguste Kerckhoffs. Onder deskundigen op het gebied van beveiliging wordt deze afhankelijkheid laatdunkend "security by obscurity" genoemd, en beschouwd als een gebrekkig ontwerpprincipe voor beveiligingssystemen. Hiervoor is een aantal redenen. Ten eerste is de algemene verwachting dat dit algoritme vroeg of laat wordt *gelekt* (bijv. door "vertrouwde" werknemers, onderaannemers of verloren documenten) of eenvoudigweg achterhaald, via reverse-engineering van de kaart. Deze laatstgenoemde methode is nu precies wat er is gebeurd met het algoritme dat wordt gebruikt in de OV-Chipkaart.

Ten tweede is het zeer waarschijnlijk dat de door CRYPTO1 geboden beveiliging, vanwege het gesloten, bedrijfseigen ontwerp ervan, slechts in betrekkelijk beperkte mate is beoordeeld. Wederom is het een breed geaccepteerde beste praktijk dat er in cryptografische systemen alleen algoritmen worden gebruikt die openlijk door cryptografische deskundigen zijn geëvalueerd. Een dergelijke beoordeling zou mogelijk bepaalde structurele zwakten blootleggen en herstellen die de ontwerpers van het algoritme (en de besloten kring van interne beoordelaars) niet hebben opgemerkt. Zo'n open beoordeling door deskundigen geeft een betere waarborg dat het algoritme sterk en veilig is.

Als we voor even de vraag laten rusten of CRYPTO1 structurele zwakten kent, betekent de onthulling van het algoritme dan per se dat de OV-chipkaarten niet veilig zijn? Hierbij hangt het antwoord af van een ander stuk informatie dat tussen de kaart en de lezer wordt uitgewisseld: een geheime sleutel. Kennis van een van de gedeelde geheimen (het algoritme van de OV-Chipkaart) hoeft niet per se te betekenen dat het andere gedeelde geheim (de sleutel) ook bekend is. Het *principe van Kerckhoffs* stelt zelfs dat een cryptografisch systeem beveiligd zou moeten blijven ook al zijn *alle* gegevens van het systeem, op de sleutel na, openbaar. Daarom zou het voor de beveiliging van de kaart *voldoende* moeten zijn als de geheimhouding van de sleutel gehandhaafd blijft. Echter, hier lopen we tegen de tweede zwakke plek van de OV-Chipkaart aan.

De geheime sleutel wordt door het algoritme gebruikt als invoer om de gegevens die worden uitgewisseld tussen de kaart en de lezer te *versleutelen* en *ontsleutelen*. De geheime sleutel is een reeks bits van een vaste lengte. Als je dus het algoritme kent en enige uitwisseling tussen een kaart en een lezer van gegevens, die met een specifieke sleutel zijn beschermd, hebt geobserveerd, dan zou je eenvoudig alle reeksen van dezelfde lengte (d.w.z. alle mogelijke sleutels) kunnen uitproberen totdat je de juiste hebt gevonden. Dit is een aanvalsvorm die kan worden toegepast op alle encryptiealgoritmen, en staat bekend als een *"exhaustive key search attack"* (aanval via uitputtend sleutelonderzoek) ofwel *"brute force attack"* (aanval met bruut geweld). Het uiteindelijke doel van een ontwerper van een cryptografisch algoritme is dat deze aanvalsvorm de meest doeltreffende aanval is op het algoritme. De ontwerper moet er vervolgens voor zorgen dat het aantal mogelijke sleutels zo groot is dat het zelfs voor een goed toegeruste aanvaller ondoenlijk is om een geheime sleutel via zo'n uitputtend onderzoek te achterhalen.

Sleutels zijn in wezen bitreeksen van een bepaalde vaste lengte (laten we zeggen: *n*). Er zijn dus net zoveel sleutels als bitreeksen met de lengte *n*. Dus als *n=l*, dan zijn er slechts twee sleutels mogelijk: 0 en 1. Als *n=2*, dan zijn er vier sleutels mogelijk, namelijk 00, 01, 10 en 11. Als *n=3*, dan zijn de acht volgende sleutels mogelijk: 000, 001, 010, 011, 100, 101, 110 en 111. In het algemeen zijn er voor elke *n* 2^n verschillende n-bitreeksen en dus 2^n mogelijke sleutels.

Het algoritme van de OV-Chipkaart maakt gebruik van sleutels met een lengte van 48 bits. Er zijn dus 2^{48} mogelijke sleutels, wat bij benadering $3x10^{14}$ is (d.w.z. het cijfer 3 gevolgd door veertien nullen). Dit lijkt een erg groot getal en een aanval met bruut geweld zou (gemiddeld) bijna alle 48-bitreeksen

moeten uitproberen voordat de juiste sleutel is gevonden. Dat lijkt onmogelijk, maar het is in de praktijk betrekkelijk eenvoudig te doen met voor dat doel gebouwde computerapparatuur die is uitgerust met hedendaagse technologie. Ter illustratie noemen we hier een bekend cryptografisch algoritme genaamd de Data Encryption Standard (DES), dat tot voor kort

door de Amerikaanse overheid als standaard werd gebruikt en algemeen werd toegepast door zowel de overheid als in het bedrijfsleven. Nu wordt dit algoritme beschouwd als verouderd, omdat er enkele jaren geleden een aanval in de praktijk werd gedemonstreerd die via een uitputtend sleutelonderzoek de gebruikte 56-bitssleutel kon achterhalen. Het zij opgemerkt dat er 256 maal zoveel DES-sleutels in omloop zijn dan CRYPTO1-sleutels (want $2^{56} = 256 \times 2^{48}$) en hoewel de specifieke bijzonderheden van de aanval op DES niet rechtstreeks van toepassing hoeven zijn op CRYPTO1, mag toch in redelijkheid worden aangenomen dat een uitputtend sleutelonderzoek op het CRYPTO1-algoritme goed uitvoerbaar is.

Daarbij zijn er andere vormen van optimalisatie die zouden kunnen worden gebruikt om een aanval met bruut geweld sneller te doen verlopen. Er heerst brede overeenstemming dat de sleutellengte die wordt gebruikt voor het algoritme van de OV-Chipkaart naar tegenwoordige maatstaven simpelweg te kort is. De meeste hedendaagse cryptografische algoritmen maken gebruik van sleutellengtes tussen de 80 en 256 bits (de opvolger van DES, AES genaamd, gebruikt sleutellengtes van 128, 192 en 256 bits). Dit is misschien wel de meest duidelijke zwakke plek in het algoritme dat voor het OV-Chipkaartsysteem wordt gebruikt. Met zo'n korte sleutellengte is de doeltreffendheid van de beveiligingsmaatregelen die door de kaart zelf worden verschaft op zijn hoogst beperkt.

Helaas is de korte sleutellengte niet het enige probleem voor CRYPTO1. Er lijkt namelijk nog een ander zwak punt te zijn. Resultaten uit onderzoek dat heeft plaatsgevonden nadat het cryptografisch algoritme van de OV-Chipkaart op straat kwam te liggen, lijken te suggereren dat CRYPTO1 inderdaad structurele zwakten vertoont die zodanig kunnen worden uitgebuit dat de beveiliging van de kaart in gevaar komt. Dit duidt op verbeterde aanvalstechnieken die veel doeltreffender zijn dan een uitputtend sleutelonderzoek.

Willekeurige getallen

Een andere zwakte die in de onlangs gehouden openbare presentatie werd aangetoond is niet rechtstreeks verwant aan het CRYPTO1-algoritme, maar heeft veeleer betrekking op de wijze waarop het algoritme wordt gebruikt in het protocol tussen de kaart en de lezer. Naast de geheime sleutel (en de boodschap), maakt het algoritme gebruik van twee andere gegevens: de herkenningscode van de kaart en een getal R, dat bij elke nieuwe transactie opnieuw wordt gegenereerd en wordt gebruikt om ervoor te zorgen dat het algoritme zich, telkens als het gegevens in het beveiligingsprotocol versleutelt/verwerkt, anders gedraagt. Dit is met name van belang voor de bescherming tegen de aanvalsvorm die bekend staat als *"replay attack"* (aanval door opnieuw af te spelen). Hierbij herhaalt een aanvaller, mogelijk de houder van een authentieke kaart, een eerdere uitwisseling van gegevens tussen de kaart en de lezer, waarbij het mogelijk is om de gegevens op de kaart (bijv. het reissaldo) op frauduleuze wijze te wijzigen.

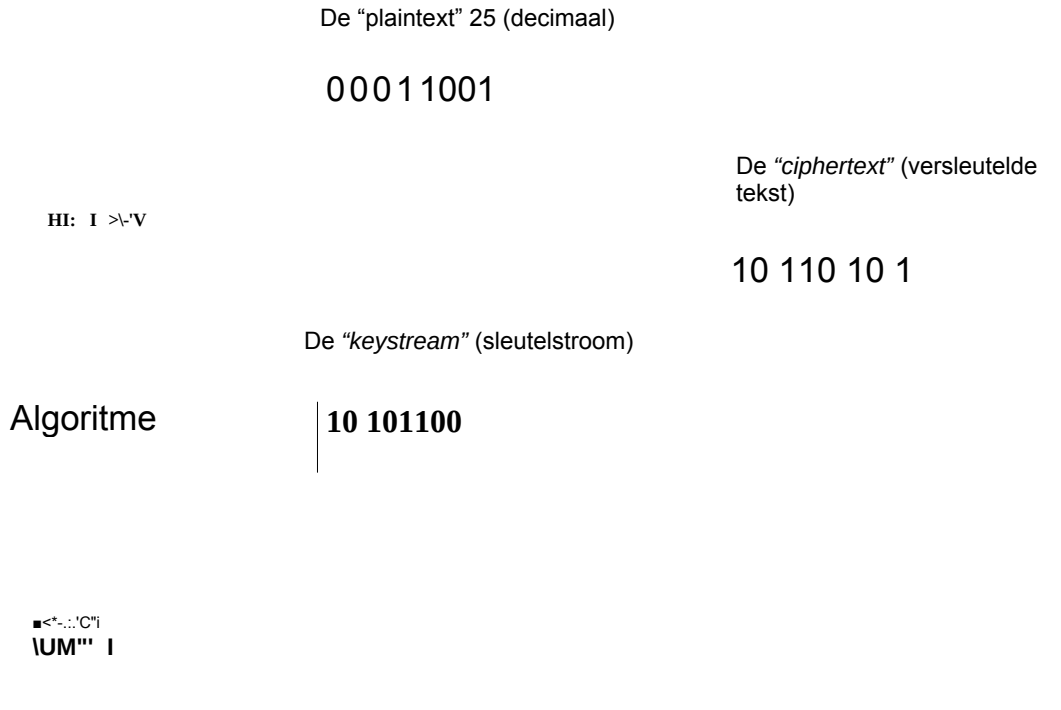
Je zou dus willen dat dit getal R *willekeurig* is, d.w.z. in essentie onvoorspelbaar en moeilijk te raden. Echter, de onderzoekers die reverse-engineering hebben uitgevoerd op het cryptografisch algoritme van de Mifare Classic-kaart deelden mee dat dit getal R relatief weinig variaties kende en dat het met een zorgvuldige timing mogelijk is om controle te hebben over de generatie van het "willekeurige" getal dat telkens wordt gebruikt, waardoor dit getal vrijwel geen bescherming meer biedt tegen aanvallen.

De realiteit van aanvallen

Eerder hebben we reeds opgemerkt dat er niet zoiets bestaat als een 100%-zekerheid en dat in principe elk doelwit kan worden aangevallen als er maar genoeg tijd, deskundigheid, middelen en motivatie aanwezig zijn. Aanvallen worden zorgwekkend als deze aantoonbaar in de praktijk zijn te brengen met beschikbare apparatuur. Nog zorgwekkender wordt de situatie als er voor de aanval minder tijd, deskundigheid en aanschafkosten van de apparatuur benodigd zijn. De aanval met bruut geweld is weinig subtiel maar effectief met behulp van bekende apparatuur. Het is voor deskundigen dan ook niet de vraag of een aanval mogelijk is, maar of er goedkopere en snellere alternatieven voorhanden zijn. Desondanks hoeft het feit dat een aanval praktisch uitvoerbaar is niet per se te betekenen dat een poging daartoe de moeite waard is (afgezien van proof-of-concept-demonstraties). De echte test komt wanneer de opbrengst van een criminele aanval op het systeem hoger is dan de kosten en inspanningen van zo'n aanval en uiteraard de pakkans. Daarom is bij een vervoerssysteem de prijs van kaartjes een belangrijke factor. Hoewel sommige seizoenkaarten erg prijzig kunnen zijn, moet men eerder uitgaan van fraude bij dagelijkse reizen. Een vervalste seizoenkaart zal immers niet voor duizenden euro's verkocht kunnen worden als deze binnen enkele dagen onbruikbaar kan worden gemaakt. We moeten ons realiseren dat vervoerssystemen nooit helemaal weerloos zijn, ook niet als ze een interessant doelwit vormen en zelfs als niet meer vertrouwd kan worden op de kaartalgoritmen. Vele jaren hebben exploitanten van vervoerssystemen te maken gehad met "inventieve" personen die proberen te frauderen. Ook zijn er vele detectie- en correctiemaatregelen in de back-office aanwezig waarmee dergelijk misbruik kan worden beperkt, ook in het geval van simpele papieren kaartjes en kaartjes voorzien van een magnetische strook. Natuurlijk zijn deze laatste verdedigingslinies niet ontworpen om een aanhoudende technische aanval te weerstaan. Daarom is het uiteraard de beste tactiek om geschikte technologie voor smart cards te gebruiken die alle voorziene aanvallen het hoofd biedt.

BIJLAGE A

De uitleg die in de hoofdtekst van deze korte inleiding wordt gegeven zou de meeste lezers voldoende opheldering moeten verschaffen. Sommige lezers is het wellicht opgevallen dat CRYPTO1 wordt omschreven als een “bitstroomencryptie” en zijn wellicht nieuwsgierig naar de betekenis daarvan. Afbeelding 1 toont een vereenvoudigd voorbeeld van zo’n encryptie.



Afbeelding 1: Vereenvoudigd voorbeeld van een bitstroomencryptie

Wat we in afbeelding 1 willen versturen kan worden beschouwd als een informatiestroom die uiteindelijk wordt weergegeven door een bitstroom met de waarde 0 of 1. Dit wordt ook wel de *plaintext* (originele boodschap) genoemd. In het voorbeeld hebben we laten zien hoe het getal 25 eruit kan zien in een binaire reeks. Om te zorgen dat een aanvaller onze reeks nullen en enen niet kan zien (en zo niet kan zien dat we het getal 25 versturen) voegen we de stream toe (op een zeer eenvoudige bit-gewijze manier[2]) aan iets dat we de *keystream* noemen. De keystream is gegenereerd door ons algoritme, dat daarvoor een aantal gegevens gebruikt waaronder de geheime sleutel. De daaruit resulterende uitvoerbitstroom die naar de lezer wordt overgedragen (de *ciphertext*) kan niet langer als onze *plaintext* worden herkend. Een aanvaller zou daarom niet moeten kunnen bepalen welke informatie is verstuurd. Het leesapparaat kent het algoritme en de sleutel ook en kan dus dezelfde *keystream* genereren die is gebruikt bij het versleutelen van de boodschap. Als de *keystream* opnieuw aan de ciphertext wordt toegevoegd, wordt de *plaintext* weer herkenbaar.

2 Het toevoegen van (XOR) gebeurt bit per bit, d.w.z. als we 0+0 toevoegen of 1+1, dan is het resultaat 0. Als we 0+1 of 1+0 toevoegen, dan is het resultaat 1.