HC 6, 12-03-2019, Inleiding cryptografie

Wat is cryptografie?
Cryptografie is de versleuteling van berichten. Daarbij heb je een kastje van versleuteling en een kastje van ontsleuteling. De veiligheid hiervan blijft staan, omdat de ontsleuteling geheim blijft. Je kan het ook omdraaien door manier van versleutelen geheim maken en de manier van ontsleutelen openbaar maken. Daardoor weet je zeker dat het bericht van de juiste persoon afkomstig was.

Het mechanisme van versleutelen en ontsleutelen heet cryptografie. Met cryptografie kun je verschillende dingen waarborgen:

- Vertrouwelijkheid
- Integriteit
- Authenticiteit

Geschiedenis
Een vorm van versleuteling is *Caesar's cipher*. Daarbij vervang je iedere letter in het bericht met de derde daar op volgende letter in het alfabet. Je vervangt de a voor de d, de b voor de e, etc. Dit kan je ontsleutelen door iedere letter te vervangen in het codebericht met drie letters eerder in het alfabet. Dit wordt ook wel **monoalfabetische substitutie** genoemd.
Extreem onveilige manier om verschillende redenen:

- Je kan informatie over de structuur van de taal gebruiken om te achterhalen wat er staat.
- Bepaalde letters komen veel voor (letterfrequenties). Daarmee kan je dus gokken.

Veiligere methodes zijn:

- **Codebooks**: woorden vervangen door andere woorden.
- Meerdere letters tegelijk vervangen door een willekeurig gekozen andere combinatie van letters.
- **Transpositie**: geen letters vervangen door andere letters, maar de letters in het bericht door elkaar gooien volgens een vaste methode van plek.
  - Een voorbeeld:

  Juliuscaesarisgek
  - Breek regel af na vast aantal letters, bijvoorbeeld 6:

  Julius
  Caesar
  Isgek
  - Zet vervolgens de letters per kolom achter elkaar:

  Jciuaslegiseuaksr

Basisgereedschap
Het *Kerckhoff's principe* houdt in dat het ontwerp van een systeem niet geheim mag zijn, want je moet ervanuit gaan dat welk systeem je ook gebruikt, componenten ervan in handen van de vijand zullen vallen. De vijand zal dus weten hoe het systeem werkt. De manier van communiceren valt dus volgens hem altijd in handen van de vijand.
→ Ga er vanuit dat het mechanisme van de versleuteling en ontsleuteling openbaar is. Hoe kun je dan alsnog garanderen dat je veilig communiceert? Door te zorgen dat de werking van die kastjes wordt beïnvloed door een cryptografische sleutel die geheim is. Die sleutels moeten bij elkaar horen. Je kan dus alleen met een goede sleutel het bericht ontsleutelen.

Vormen van cryptografie:

1. **Symmetrische cryptografie**: sleutel van verzender is dezelfde als de sleutel van de ontvanger. Voordeel hiervan is dat de versleuteling snel gaat en dat de sleutel die je gebruikt relatief kort is. Voorbeelden hiervan zijn Data Encryption Standard (DES) en Advanced Encryption Standard (AES). Bij AES werd het standaardisatieproces openbaar gemaakt (dus volgens het kerkhoff's principe).

Als je doormiddel van symmetrische cryptografie een bericht wil versturen. Moeten verzender en ontvanger een symmetrische sleutel afspreken en die beiden geheim houden. Vervolgens versleutelt de verzender het bericht. Daarna kan de ontvanger het bericht weer ontsleutelen met die symmetrische sleutel.

Voordelen
- Korte sleutels
- Snelle versleuteling en ontsleuteling

Nadelen
- De veiligheid is niet sterk theoretisch onderbouwd, in de praktijk is dit geen probleem.
- Sleutelbeheer: hoe spreek je met iemand op een veilige manier een sleutel af als je niet fysiek op dezelfde plek bent?
- Sleuteldistributie: voor ieder persoon waarmee je wil communiceren, heb je een andere sleutel nodig. Anders kunnen al die personen ook de berichten lezen die je naar anderen verstuurt of van anderen ontvangt.
- Sleutel moet geheim blijven: de sleutels opslaan op je hard drive o.i.d. is niet erg handig.

2. **Assymetrische cryptografie**: er wordt gebruik gemaakt van een publieke sleutel en een geheime sleutel, waarbij de geheime sleutel wordt gebruikt om berichten te ontsleutelen en de publieke sleutel wordt gebruikt voor de versleuteling van het bericht.

Nadelen
- Traag
- Sleutels zijn erg lang

Voordelen
- Veiligheid is gebaseerd op wiskundige theorie.
- Eenvoudige sleuteldistributie: je hoeft maar één privésleutel te onthouden.

Verschil symmetrische en asymmetrische cryptografie
Bij symmetrische cryptografie spreek je samen één sleutel af die aan beide zijden geheim is. Bij asymmetrische cryptografie is er niet meer sprake van één sleutel, maar twee sleutels. De publieke sleutel van de ontvanger moet daarbij worden opgezocht, deze is immers openbaar. Vervolgens versleutelt de verzender met de geheime sleutel het bericht. Het asymmetrische systeem maakt dus gebruik van bij elkaar horende sleutels: een publieke sleutel en een privé sleutel. Deze worden tegelijkertijd gegenereerd. Met de publieke sleutel kan de privé sleutel niet worden uitgerekend.

Versleutelen in de praktijk
- Genereer een willekeurige symmetrische sleutel
- Versleutel het bericht met die sleutel
- Zoek de publieke sleutel van de ontvanger op
- Versleutel met die publieke sleutel
- Stuur het versleutelde bericht met publieke sleutel naar de ontvanger

Ontsleutelen van dit bericht
De ontvanger heeft de privésleutel waarmee hij het bericht kan ontsleutelen. Vervolgens ontsleutelt hij dat weer met de publieke sleutel.

Integriteit: hashfunctions
Hashfunctie is een functie die gegeven een willekeurige invoer, een hashcode uitrekent die uniek is voor die invoer. Dit werkt one-way: het is andersom onmogelijk om de invoer te berekenen. De toepassing van hashfuncties kan op een aantal manieren:

1. Integriteit beschermen door de hash van een boodschap direct achter de boodschap te zetten.
2. **Timestamping**: de hash van een document bijvoorbeeld in de New York Times zetten. Zo leg je vast dat een document op een bepaald tijdstip bestond zonder document vrij te geven.
3. Hashing in de blockchain.

Veiligheid
Als je een bericht wil ontcijferen, is de enige mogelijkheid die je hebt om alle mogelijke sleutels te proberen. Daar om is de sleutellengte bij cryptografie erg belangrijk, computers worden namelijk steeds sneller maar ook voor een computer wordt het te veel om een oneindig aantal mogelijkheden uit te proberen. Toch zijn veel ciphers niet goed, denk daarbij bijvoorbeeld aan autosleutels, chipkaarten etc.

Als je cryptografie naïef toepast, zijn er een aantal valkuilen:

- Hetzelfde bericht met dezelfde sleutel versleuteld heeft dezelfde ciphertext. Als je geen goede beveiligingsmaatregelen neemt, dan zou dat betekenen dat mensen mogelijk niet kunnen zien wat erin staat, maar wel dat het gelijk is aan een eerder bericht.
- Een hashfunctie is niet inverteerbaar. Maar je kunt wel testen of je vermoeden van een mogelijke invoer juist is. Ook kun je een woordenboek maken met voor ieder kenteken de hash van dat kenteken, gesorteerd op de uitvoer.

Hashfuncties zijn dus alleen maar veilig als de invoer uit een voldoende grote verzameling mogelijkheden komt.

Toepassingen
End-to-end encryption
Als jij een bericht stuurt naar een van je vrienden via WhatsApp, versleutelt jouw telefoon het bericht en verstuurt het via de server naar de ontvanger, waar het bericht weer wordt ontsleutelt (met bijbehorende privésleutel). Whatsapp genereert bij de download het sleutelpaar. De privésleutel houd je zelf en de publieke sleutel wordt opgeslagen op de browser van WhatsApp. Dit wordt ook wel end-to-end encryption genoemd. Omdat tussenliggende partijen niet de beschikking hebben over die privésleutel, kunnen zij deze berichten niet lezen. Het heeft voor hen geen zin om de berichten te onderscheppen. Om het te kunnen lezen, moet worden ingebroken op de telefoon van de persoon zelf.

Opslaan van documenten in de cloud
Twee manieren waarop documenten kunnen worden opgeslagen in de cloud:
Cloud provider heeft de sleutel
Als je document wil opslaan in de cloud, versleutel je het voordat je het naar de cloud stuurt. Als het bij de cloud-provider komt, wordt het ontsleuteld en vervolgens weer versleuteld met de sleutel die de cloud-provider heeft. De berichten zijn dus versleuteld, maar de cloud-provider kan ze ten alle tijden ontsleutelen. Als al je apparaten stuk zijn, maar je hebt nog wel de inloggegevens van je cloud, dan kun je alsnog bij die documenten.

Gebruiker heeft de sleutel
Je versleutelt het document met je eigen sleutel, cloud-provider slaat het document op zoals jij het hebt versleuteld. De cloud-provider kan dit dus niet ontsleutelen, want alleen jij hebt de sleutel. Een groot nadeel hiervan is dat als je computer stukgaat waar die sleutel opstaat, dan ben je het document in de cloud kwijt. Voordelen zijn beveiliging en privacy.

Een digitale handtekening
Voor het zetten van deze handtekening gebruik je de privé sleutel, voor het verifiëren moet je de bijbehorende publieke sleutel gebruiken. Iedereen kan de handtekening dus verifiëren. Het zetten van de digitale handtekening kan dus maar door één persoon. Bij een **praktische handtekening** zet je de

handtekening door middel van een hash. Dan dient bij het verifiëren van de handtekening weer dezelfde hash te worden gebruikt.

Trusted Third Parties
Trusted Third Parties zijn entiteiten die, op basis van vertrouwen door andere partijen, diensten aanbiedt ter beveiliging van de communicatie of handelingen tussen deze partijen. Als je een versleuteld bericht naar een ander wil sturen moet je de publieke sleutel hebben van de ontvanger. Een vorm van sleuteldistributie is een TTP die de publieke sleutels van iedereen kent en die doorgeeft. Als je dan een bericht wil sturen, kun je die publieke sleutel van de ontvanger opvragen bij de TTP. Als de ontvanger een nieuwe sleutel krijgt, moet hij dit doorgeven aan de TTP (sleutelregistratie). Dit gebeurt dus allemaal online.

Dit kan ook offline door middel van **certification authorities**. In plaats dat de TTP de publieke sleutel opslaat, geeft de TTP (CA) je een certificaat versleuteld met een privé sleutel om de certificaat mee te ondertekenen. Dat certificaat bevat de naam, de sleutel en een digitale handtekening van diegene. Als je de publieke sleutel van diegene wil hebben, kun je dat aan de ontvanger vragen. De ontvanger kan het certificaat opsturen. Daarmee is de verzender ervan verzekerd dat dit de publieke sleutel van de juiste persoon is.