Week 6

Week 6A inleiding cryptografie

Cryptografie is een versleuteling van een bericht, ook wel de plain text genoemd, zodat de inhoud niet leesbaar is voor een onderschepper van het bericht, tenzij diegene de sleutel in zijn bezit heeft om dit bericht weer te ontsleutelen. Het versleutelen van deze berichten kan op 2 manieren plaats vinden.

- Symmetrische cryptografie, in deze vorm van cryptografie hebben zowel de zender als de ontvanger dezelfde sleutel.
- Asymmetrische cryptografie, in deze vorm van cryptografie gebruikt de zender een publieke sleutel en de ontvanger een privé sleutel die alleen hij kan gebruiken.

Vanuit de geschiedenis zijn er verschillende versleutelingen bekend, zoals de 'Caesar's cipher' waarin elke letter in het alfabet werd vervangen door er 3 letters bij op te tellen, A werd dus D. Deze vorm van versleutelen heet **mono alfabetische substitutie**. Een simpele vorm van cryptografie die hedendaags niet veilig zou zijn.

Enkele manieren om dergelijke methodes toch veiliger te maken:

- Codebooks, waarin je complete woorden vervangt door een codewoord
- Meerdere letters tegelijk vervangen, echter in de praktijk erg onpraktisch
- Geen substitutie maar transpositie (permutatie), een vaste methode toepassen om letters te wisselen in een woord.

Het hierboven genoemde voorbeeld is een klassieke vorm van symmetrische cryptografie, de versleuteling en ontsleuteling geschied met hetzelfde mechanisme. Hoewel makkelijker te kraken zitten hieraan ook voordelen, doordat partijen dezelfde sleutel gebruiken is het sleutel proces een stuk sneller, mede door het feit dat een sleutel relatief kort is (128-256 bites). De nadelen spreken voor zich, de afgesproken sleutel moet geheim blijven anders kan iedereen het bericht lezen.

Om dit nadeel op te lossen is er Asymmetrische cryptografie bedacht. Dit werkt trager, iedereen verstuurt een bericht d.m.v. de publieke sleutel, wanneer jij dit bericht binnen krijgt kan alleen jij hem ontcijferen omdat de ontvanger de private sleutel heeft die gekoppeld is aan die publieke sleutel om te kunnen ontcijferen. Als verzender hoef je dus niet bang te zijn voor onderschepping omdat je altijd de private sleutel nodig hebt om te kunnen ontcijferen, de sleutels zijn ook langer (1024-2048 bites).

Ter illustratie van asymmetrische cryptografie, een bericht wordt verstuurd in een kist die wordt afgesloten met een hangslot. Het hangslot is de publieke sleutel die alleen geopend kan worden door de private sleutel die bij dit hangslot hoort. Op deze manier kan degene die het bericht in de kist heeft verzonden er zeker van zijn dat de kist bij onderschepping niet geopend kan worden.

Hash functions

Berichten kunnen ook versleuteld worden d.m.v. hash functions, hier wordt een groep waarden omgezet in een andere vorm, de uitkomst wordt Hash genoemd. Dit is handig omdat je op deze manier grote hoeveelheden data kan samenvoegen tot één hash wat uiteindelijk minder opslagplek nodig heeft.

Kenmerken

- x = y dan h(x) = h(y)
- One way, wanneer c=h(x) gegeven is, is het onmogelijk om x te berekenen
- Collisison resistance: het is onmogelijk om een bericht te vinden dat is versleuteld met dezelfde hash code
- Hash code is 128-256 bits lang, een bekend voorbeeld is SHA-256 (gebruikt bij bitcoin)

Week 6b toepassingen cryptografie

Toepassingen van hash functies

Integriteit beschermen (tegen toevallige fouten)

- Zet de hash h(m) van een boodschap direct achter de boodschap, dit resulteert in het volgende, wanneer het bericht is aangepast komt het niet meer overeen met de hash functie

Timestamping

- Zet de hash van een document in de New York Times, op deze manier leg je vast dat een document op een bepaald tijdstip bestond, dit kan relevant zijn bij conflicten over een patent.

Blockchain

Een datastructuur, waarin je een aantal transacties in een blok zet met een verwijzing naar oudere transacties. Zo kan dus alle oude transacties met bijvoorbeeld Bitcoin worden teruggehaald. Belangrijk is dat er niets gewijzigd kan worden in deze blocks, vandaar dat ook in blockchain gebruik wordt gemaakt van hash functies.

Valkuilen

Hetzelfde bericht met dezelfde sleutel heeft dezelfde ciphertext.

- Dus, hoewel je niet kan zien wat de inhoud is, kan je wel redeneren
- De vorige keer dat we zo'n bericht zagen viel het leger aan, dus…

Een hash functie is niet-inverteerbaar

- Maar je kunt wel testen of vermoeden of een mogelijke invoer van x juist is. Dit brengt dus mee dat je voor het gebruik van hash functies een grote verzameling mogelijke uitkomsten hebt.
- Wanneer de tabel niet zo groot wordt kan je dus alsnog inverteren.

Toepassingen

End to end encryptie

WhatsApp verstuurt een versleuteld bericht, wat bij facebook versleuteld wordt opgeslagen (tot dat je online bent), en wanneer het appje binnen komt wordt ontsleuteld.

De cloud versleuteling, dit kent 2 manieren:

1. Cloud provider heeft de sleutel, hierin wordt het bericht versleuteld naar de cloud gestuurd waar het bericht wordt ontsleuteld om vervolgens door de cloud service weer versleuteld te worden. Dit heeft als voordeel wanneer je als gebruiker de sleutel kwijtraakt je met je wachtwoord en inlognaam nog steeds bij de berichten kunt, immers heeft de provider de sleutel.
2. Gebruiker heeft de sleutel, via deze manier worden berichten versleuteld opgeslagen in de cloud. Dit is een stuk veiliger omdat niemand erbij kan, echter heb je wel een probleem wanneer je geen back-up van de sleutel hebt en die kwijtraakt.

Een digitale handtekening

Je draait hierbij de rol van de sleutels bij asymmetrische versleuteling om. Met de private sleutel zet je een handtekening onder een bericht, vervolgens wordt de publieke sleutel gebruikt om te verifiëren. Ook hierin wordt gebruik gemaakt van een hash functie, het bericht wordt d.m.v. een hash functie omgevormd waar je dan een digitale handtekening opzet.

Trusted third parties

Online:

Een belangrijke rol in de cryptografie zijn derde partijen, aan deze partijen worden de publieke sleutels toevertrouwt. Via sleuteldistributie kan er dus een publieke sleutel door partij x van partij y aan de derde partij wordt gevraagd, x stuurt dan met de verkregen publieke sleutel een bericht aan y en deze ontsleutelt dit vervolgens met zijn eigen private sleutel.

Offline:

Hierin is de derde partij niet online, in deze context wordt de derde partij een certification authority (CA) genoemd. Tussen de derde partij en Bob is hier een sleutel registratie, waarin Bob een certificaat krijgt die ondertekent is door de CA met een publieke sleutel. Dit komt neer op een ondertekent certificaat waarin staat ‘bob’s sleutel is dit’.

Vervolgens verstuurt bob een sleutel met dit certificaat naar Alice, die met de publieke sleutel van de CA kan controleren of de publieke sleutel van Bob is.