Encryptie - Theorieles

Wat is Encryptie?

Encryption (of encryptie of versleutelen) is het versleutelen van gegevens zodat je zonder de juiste sleutel de gegevens niet kan lezen. Encryptie bestaat uit het algortime (de regels/procedure van de encryptie) en een of meer sleutels.

Voorbeeld van encrypted data.

```
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALhzGuSqLXPRAz1MJzhvTdHMTCTp
tkvusbSVmVRTL7YmW5ICIW570+8uzQX5+16KoXT/B5s5ZnNgTq9VvmrAbjuHw+bL
dQnB+SPRdg9vKTfJOWRLonyCzKS9T/wSVW9yTPuaol2++4HR6LF2P2ifwvgj1aq2
UYZXcu2TmgdDMA+JXyREV8kRRnXxUbaeq6+2Ypnl1+0qIGqAL3mWpZ5CC1/nWCIR
vMi0ASOwYPnjcu86FwIcf/24hoHFsdp2eKosI+IoV23JXGhhXeKKROeEz85kezpx
```

Decryption (of decryptie of ontsleutelen) is het weer leesbaar maken van encypted data.

Waarom Encryptie?

Encryptie is belangrijk omdat het kan helpen voorkomen dat informatie in verkeerde handen valt.

Stel je krijgt toegang tot de database van Facebook en je kunt alle logins en passwords lezen. Dat zou heel vervelend zijn, maar het is iets minder vervelend als de wachtwoorden zijn versleuteld en het zou nog minder erg zijn als alle gegevens zouden zijn versleuteld. Of stel je telefoon of laptop word gestolen. Vervelend, maar als je gegevens op de harddisk (of SSD) zijn versleuteld kan niemand jouw gegevens lezen.

Door encryptie worden bijna alle risico's op de threats uit het STRIDE model verminderd. Dat geld voor de threats;

> *spoofing, tampering, repudiation, confidentiality, en authorization,*

> Vraag 1: Hoe kan encryptie het risico op repudiation ('I did not send that email') helpen vermindeeren?

Encryptie is niet alleen iets van computers ; het is al 2000 jaar oud.

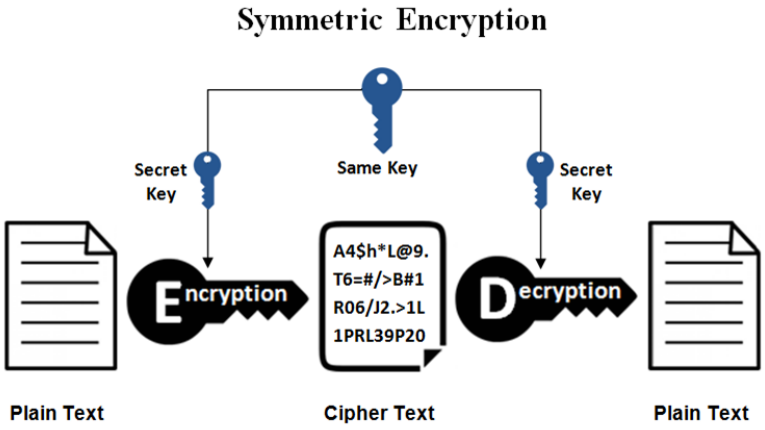
>

> Vaag 2: In welke situatie denk je dat 1000 of meer jaar geleden encryptie zou zijntoegepast? Als je niets kunt bedenken, denk eens terug aan "Game Of Thrones".

Symetrisch Encryptie

We maken onderscheid in symetrische encryptie en asymetrische encryptie.

Symetrische encryptie is eenvoudig en al heel oud. De meest eenvoudige vorm is het omzetten van elke letter in een ander letter. Je kunt letters verschuiven, maar je kunt het ook ingewikkelder maken. In de klas hebben we geoefend met Caesar encryptie.



Symetrisch encyptie is redelijk eenvoudig en daardoor ook realtief makkelijk en efficiënt op een computer te implementeren. Er is ook een groot nadeel:

> Bij symetrische encryptie moet je een sleutel uitwisselen en je moet daarbij voorkomen dat de sleutel in verkeerde handen valt.

PKI, Public Key Infrastructure

Het nadeel van het lastig uitwisselen van de key bij symetrische encryptie wordt opgelost bij PKI, *Public Key Infrastructure.*

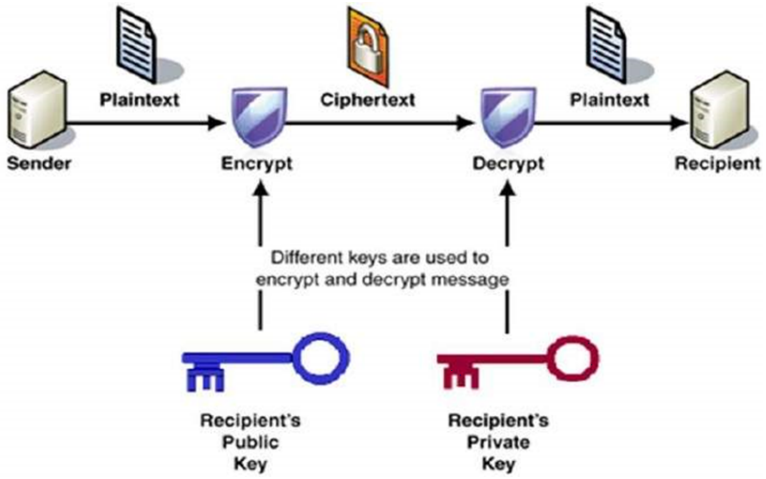
PKI, is een systeem met twee sleutels: de public key en de private key (de publieke sleutel en de privé sleutel).

De public key kan je verspreiden, iedereen mag hem hebben, want je kunt er alleen een bericht mee versleutelen. Je kunt er geen bericht mee ontcijferen/lezen. Alleen met de bijbehorende private key kan het versleutelde bericht worden gelezen.

In de les hebben we dit zichbaar gemaakt met een (open) hangslot en de sleutel. Het open hangslot was de public key en die kon iedereen krijgen. Je kunt dan een boodschap sturen en

alleen degene met de sluetel van het hangslot kan dan het bericht ontcijferen.

Of iets formeler (en let op: als we het over security en encryptie hebben dan hebben we het altijd over Alice en Bob).
Stel, Alice wil een bericht sturen aan Bob. Bob is in het bezit van een publieke sleutel en een privésleutel. Alice ontvangt dan de publieke sleutel van Bob. Hiermee versleutelt zij het bericht en daarna verstuurt ze het naar Bob. Bob ontsleutelt het bericht met zijn privésleutel en kan het dan lezen.



Dus je geeft idereen die dat wil je public sleutel en iedereen die dat wil kan een bericht versleutelen en jij bent de enige die met de private key het bericht kan ontsleutelen.

Of stel dat jij een wachtwoord wilt instellen op www.lekkergoedkoop.nl dan kun je met de public key van deze site je wachtwoord versleutelen en je weet dan zeker dat alleen de site www.lekkergoedkop.nl jouw versleutelde wachtwoord kan lezen. Maar is dat wel zo? Wat nu als je denkt dat je op de site www.lekkergoedkoop.nl zit maar via een slinkse manier (DNS Spoofing, Host file manipulatie, Phissing) op een andere site terecht ben gekomen. Je denk dat je je wachtwoord naar www.lekkergoedkoop.nl stuurt maar het is een hele ander site. Hoe weet je nu zeker dat je de public key van de echte site hebt gekregen?

Certificaten

Een certificaat is digitaal ondertekend versleuteld document dat is uitgegeven door een Certified Authority. Je kunt het zien als een diploma dat is uitgegeven door een school. Niet iedere school mag zo maar een diploma uitreiken. Een digitaal certificaat mag ook alleen worden uitgegeven door bepaalde instanties en via bepaalde web sites.

Als ik nu een site heb en ik wil dat de gebruiker een public key krijgt zodat wij veilig kunnen communiceren, dan kan ik deze public key via een certificaat uitdelen. Dit certificaat verklaart dan dat ik ben wie ik zeg dat ik ben en het certificaat bevat mijn public key.

Bij het aanvragen van een certificaat bij een CA, Certified Authority, wordt gecontroleerd wie jij bent en of jij een betrouwbare partij bent. Een certificaat heeft altijd een bepertke houdbaarheiddatum en zal dus na verloop van tijd moeten worden vernieuwd.

Dus nu kunnen we naar een website en kunnen we al het verkeer tussen mijn computer en de web server versleutelen via de private key die ik via een certificaat heb ontvangen. Alles opgelost of niet?

SSL

SSL staat voor **Secure Socket Layer** en het is standaard manier om verkeer tussen jouw browser en de webserver te versleutelen. Zodra er een SSL verbinding is opgezet tussen jouw browser en de webserver dan zie je een slotje of ander icoontje wat aangeeft dat je een veilige verbinding hebt. Ook veranderd het begin van de URL van HTTP in HTTPS.



Het opzetten van een veilige (=versleutelde) veriding kunnen we dat het beste doen via PKI waarbij de public key via een certificaat wordt opgevraagd. Maar PKI is complex en daardoor traag, als we al het verkeer telkens via PKI willen encrypten en decrypten dan gaat dat al snel voor vertraging zorgen. Symetrische encrypty is veel sneller maar daarbij was het probleem dat we niet eenvoudig de sleutel konden verspreiden.

De oplossing is de combinatie van beide technieken.

We gebruiken PKI om een tijdelijke symetrische sleutel uit te wisselen die we daarna gebruiken voor al het SSL verkeer. Dus we gebruiken de 'trage' PKI methode om ervoor te zorgen dat we op een veilige manier de *symetrische* sleutel uitwisselen. Vanaf het moment dat de browser en de web server allebij dezelfde symetrische sleutel hebben kan het verkeer via symetrische encrypty veilig en snel worden opgezet. Zodra de web sessie eindigt (via uitloggen of via een time-out) wordt de symetrische key ook weggegooid en bij de volgende sessie wordt er een nieuwe symetrische sleutel uitgewisseld via PKI. Door telkens een neiuwe symetrische sleutel te gebruiken verlaag je de kans dat deze key uitlekt en door een hacker kan worden misbruikt.

In het kort: SSL en het Slotje geven aan dat de website is beveilgd met een SSL certificaat. SSL is alleen tegenwoordig eigenlijk TSL.

TSL

TLS staat voor **Transport Layer Security** en is een verbeterde en veiligere versie van SSL. Met de ontwikkeling van TLS zijn vele kwetsbaarheden die voorkomen in oude SSL protocollen verholpen en zijn nieuwe beveiligingsmechanismen toegevoegd. In de praktijk wordt eigenlijk allees TSL nog gebruikt maar we nomen het nof vaak SSL.

Vragen

1. In welke situatie denk je dat 1000 of meer jaar geleden encryptie zou zijn toegepast? Als je niets kunt bedenken, denk eens terug aan "Game Of Thrones".

2. Hoe kan encryptie het risico op repudiation ('I did not send that email') helpen verminderen?

3. Hoe kan encyptie het risico op tampering verminderen?

4. Noem een voorbeeld waarbij het niet erg is om een via een niet beveiligde verbinding (niet SSL) een web site te bezoeken.

5. Als je je wachtwoord op een site veranderd dan moet je je oude en nieuwe wachtwoord opgeven. Is het dan van belang om dit via een SSL verbiding te doen? Leg uit waarom!

6. Waar staat HTTPS voor *(alle* letters benoemen)?

7. Vul bij (a), (b), (c) en (d) (zie tabel hierboven) de voor- en nadelen van symetrische en asymtrische encryptie in:

	Voordeel	Nadeel
Symetrische encryptie	(a)	(b)
Asymetrische encryptie	(c)	(d)

Revision #8
Created 2019-09-27 10:46:11 UTC by Admin
Updated 2019-09-28 14:24:47 UTC by Admin