# Public Key Cryptografie

**Symmetrische (DES, AES)**

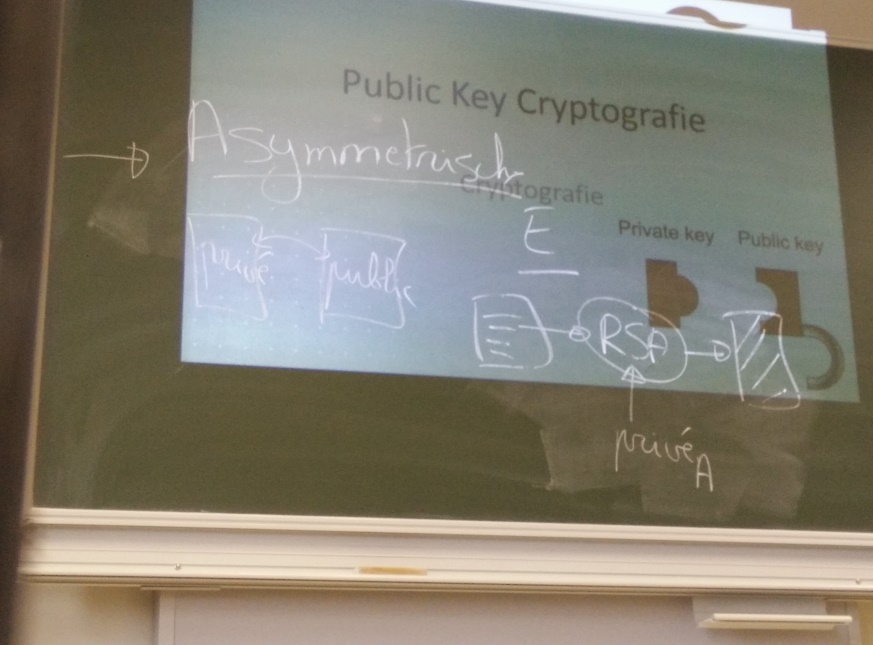
Positief: SNEL

Negatief: key management 🡪 enorm veel keys voor mensen met elkaar te laten comuniceren

**Asymmetrisch (RSA)**

Positief: Key Manegement 🡪 enkel uw eigen prive sleutel moet ge managen

Negatief: TRAAG



**4 wisk magic**

**Welk algoritme maakt daar gebruik van? (EXAMEN)**

* RSA , Factorisatie 🡪 zoek me 2 grote priemgetallen die vermenigvuldigt een getal uitkomt.
* Discrete logaritme (zolang ge log schrijft is het goed ) , Diffie-Hellman (met die kofferkes van A naar B sturen) wiskundig 🡪 Y = g^x mod(p) , G , P en Y zijn gekend, zoek X

Log(y) = log(g^x) = x log(g) 🡪 log(y) / log(g) = x

* Knapzak probleem (er zit een wiskundige zwakheid in op moment)

Ge hebt een heel warenhuis en die staan vol met items en alle items zijn verschillend , die hebben een bepaald gewicht en een bepaalde waarde. U taak ge krijgt een rugzak van max 15 kg , vul die rugzak zo optimaal mogelijk zonder dat die scheurt. (iedereen weet wat er in het warenhuis zit) Dit zijn zoveel combinaties dat ge moet uitrekenen dat het onmogelijk is om te weten wat. De truc is een key te hebben. Je geeft bepaalde items bv een diamant en een muntstuk en dan kan je de andere uitrekenen.

* ECC (Elyptische curve cryptografie)

Extreem wiskundige , extreem snel voor assymetrische cryptografie maar trager als DES of AES

**Hash**

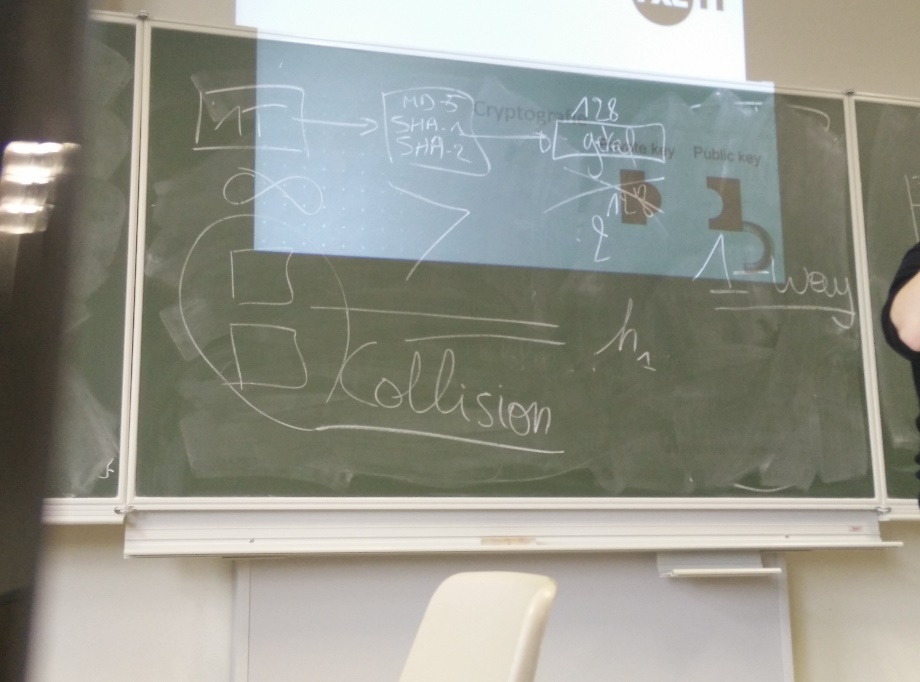
Fingerprinting techiek , kan alle soorten files aan , ge krijgt een 128 bit getalleke , als ge der maar 1 bit veranderd dan krijgt ge een volledig ander getal. Hashes wordt gebruikt voor paswoorden bij te houden.

2 files die dezelfde hash uitkomen noemt men een **Collision**

In de praktijk is hashing **collision free**

**Voor het examen :** EEN HASH IS EEN PURE **ONE WAY FUNCTION**

Ge kunt nooit een inverse hash doen !



Ik ben **een hacker** en ik zou graag iets te weten komen:

Zoek op Birthday paradox. Random mensen van straat pakken, in een lokaal stoppen en kijken of die dezelfde verjaardag hebben als u , ongeveer 253 man pakken 🡪 **Directed Attack**

Mensen van straat pakken en kijken of ze onderling dezelfde verjaardag hebben , ongeveer 23 🡪**Broad Attack**

Ze hebben een dictionary , een supergrote file , van al die paswoorden gaan ze de hashcodes berekenen. 🡪 **brute force attack 🡪** komt ge ooit het hash tegen van iemand , dan kunt ge dat gewoon invullen.

**RAINBOW TABLE ATTACK 🡪**  een dictionary zo optiaal mogelijk maken

**Hoe beveilgen? :**

Door **Salting**: Een 128 bit getal wordt bij de eerste keer inloggen , dan komt bij het paswoord + Salt opgeteld en dat wordt op de hash gezet in die tabel op de server.

Doordat ge een salt hebt kunt ge enkel een direct attack doet omdat iedereen een andere salt heeft. Dus is het bijna niet meer mogelijk om een persoon te hacken.