CySec – les 2

Algoritmes, Beveiliging, encryptie, hashing en RSA

Nova College

Programma

- Wat weten we nog?
- Algoritmes – basis
- Beveiliging
- Denk pauze
- Encryptie
- Hashing
- RSA
- Afsluiting

Leerdoelen

- Aan het einde van de les:
  - Weten we wat een algoritme is
  - Weten we welke kenmerken horen bij beveiliging
  - Weten we hoe en waar we wachtwoorden kunnen bewaren
  - Weten we wat encryptie is
  - Weten we het verschil tussen 1 en 2 richtings encryptie
  - Weten we hoe Hashing werkt
  - Weten we wat RSA is

Wat weten we nog van de vorige les?

Algoritmes

- Defenitie: een preciseze set van instructies of regels die een probleem oplost of een taak uitvoert.
- Stukken code zijn algoritmes
- Binnen de ICT wereld spreken we over algoritmes bij stapsgewijze instructies om berekeningen te maken.
- Kan simpel zijn zoals btw op boodschappen
- Kan complex zijn zoals beveiliging encryptie en decryptie

Wat is wel en niet een algoritme?

- Print “Hello world”

- Var number = 0;
  While number<10{
  number++;
  print “hello world”;
  }

- Berekenen wat de helderheid van het scherm moet zijn voor de tijd in je game wereld

Beveiliging

Pauze? – Ga maar een wachtwoord zoeken

6 delen te vinden, geef me het volledige wachtwoord om een beloning te verdienen ☺
Een hulpmiddel voor bij je examen!

Nova College

Encryptie

- Encryptie is het verbergen van betekenis in een andere onleesbare vorm. Voorbeelden zijn:
  - Een versleuteling
  - Een ander medium
  - Een verschuiving
- Taal is ook een encryptie van een soort.

2 richting encryptie

- Ook wel bekend als symmetrische encryptie.
- 1 key voor encryptie en decryptie
- Caesar, vignere en andere oudere encrypties zijn voorbeelden hiervan.

1 richting encryptie

- Ook wel bekend als asymmetrische encryptie
- 2 Keys, een publiek en een privé
- De publieke key wordt open gesteld of mee gestuurd
- De privé key is alleen beschikbaar voor de eigenaar en ontvanger
- Public key nodig voor encryptie
- Beide keys zijn nodig voor decryptie
- Voorbeelden zijn RSA, ECC en DSA

Wanneer gebruik je welke encryptie?

2 richting encryptie

- Communicatie tussen mensen
- Inhoud moet beschikbaar worden
- Keys moeten simpel zijn
- Geen cruciale data
- Brute force is makkelijker

1 richting encryptie

- Communicatie tussen mens en machine
- Inhoud moet geheim blijven
- Encryptie snelheid speelt geen rol
- Cruciale data
- Brute force neemt veel tijd

Hashing

- Hashing is vergelijkbaar met 1 richting encryptie
- Hashing is decryptbaar.
- Gebruikt voornamelijk voor wachtwoorden binnen databases
- Encryptie is snel
- Encryptie key mag publiek zijn.

RSA – 1 richting

- 2 grote priemgetallen met elkaar vermenigvuldigen, resultaat N wordt gebruikt voor de sleutels.
- We berekenen ook M, dit is (Priem A-1) X (Priem B-1)
- Kies een getal tussen 1 en M dat niet deelbaar is met M, dit is E
- Als laatste is er D, de prive key. Dit is de restant van E^-1 delen door N + 1
- Je public key is N en E
- Je private key is d

RSA – 1 richting

- 2 grote priemgetallen met elkaar vermenigvuldigen, resultaat N wordt gebruikt voor de sleutels.
- We berekenen ook M, dit is (Priem A-1) X (Priem B-1)
- Kies een getal tussen 1 en M dat niet deelbaar is met M, dit is E
- Als laatste is er D, de prive key. Dit is de restant van (E^-1 delen door N) + 1
- Je public key is N en E
- Je private key is d

Dit hoef je NIET te kennen

RSA voor het examen

- Het is een 1 richtings exncryptie
- Het maakt gebruik van 2 grote priemgetallen
- Het maakt kraken bijna onmogelijk indien de priemgetallen groot genoeg zijn
- Wordt onder andere gebruikt in SSL certificaten

Programeer opdrachten

- Kijk op de Dummymeneer GitHub voor de opdrachten van Cyber security en de slides
- Hier komen ook extra materialen op te staan om te helpen met het examen.
- https://github.com/DummyMeneer/Cyber-Security

Volgende week:

- Internationale cyber wetten
- Europese cyber wetten
- cyber awareness