Theorie week 7 – Security

Deze week werk je verder aan leerdoel 4 dat is beschreven in de cursushandleiding.

Je gaat deze les leren:

- wat cryptografie is;
- hoe cryptografie gebruikt kan worden om confidentie, data-integriteit en authenticatie bij communicatie te garanderen;
- hoe versleutelde berichten d.m.v. cryptoanalyse gekraakt kunnen worden.

Studiemateriaal week 7

De theorie die je deze week moet bestuderen kun je vinden in de volgende paragrafen van je boek[1]:

17 Security
17.1 Inleiding
17.2 Doelstellingen van de cryptografie
17.3 Geschiedenis en basisbegrippen
17.4 Wiskundige achtergrond
17.5 Symmetrische cryptografie
17.6 Asymmetrische cryptografie
17.7 Praktische realisaties
17.8 Steganografie

Verdieping

Tegenwoordig maken veel chat-applicaties gebruik van encryptie. WhatsApp claimt peer-to-peer encryptie. Maakt WhatsApp gebruik van een Public Key Infrastructure?

Wat betekent het wanneer een chat-applicatie wel geëncrypt is, maar niet peer-to-peer?

Bij het achterhalen van wachtwoorden wordt vaak een rainbow-table gebruikt. Hoe werkt dit principe?

[1] Leo van Moergestel. *Computersystemen en embedded systemen*. 4de ed. Boom, 2016. ISBN: 9-789058-754233.

Als je gebruik maakt van versleutelde mail m.b.v. asymmetrische encryptie, dan wil je een bericht dat je hebt verstuurd natuurlijk niet onversleuteld in de map 'Verzonden berichten' opslaan. Deze map bevindt zich namelijk meestal ook op de mailserver en dan is alsnog de geheime informatie niet veilig. Toch wil je het bericht misschien later nog inzien. Er is een oplossing waarbij je het bericht toch in de map verzonden berichten kunt opslaan. Zoek uit hoe dit werkt.

Opgaven week 7

7.1 De Caesarencryptie is toegepast op 'EMS20' met als resultaat 'RZF75'. Er zijn hiervoor twee sleutels gebruikt: één voor het alfabet (A-Z) en één voor de nummers (0-9).

A Wat zijn de sleutels (keys)?

B Wat zijn de cijferteksten (ciphers)?

C Waarom zijn de sleutels zo makkelijk te achterhalen? Hoe verschilt dit van een meer reële situatie?

7.2 Je ontvangt een bericht, gecodeerd met Vigenère. De sleutel was van ten voren al bekend en is *ELE*. De cijfertekst die wordt ontvangen is *KZIH RIHLER*.

A Maak gebruik van de tabel op pagina 352 van het boek, om het bericht te achterhalen. De spatie is niet gecodeerd.

B Waarom moet de sleutel van tevoren al afgesproken zijn?

7.3 Maken opgaven 7.1 en 7.2 gebruik van transpositie of substitutie?

7.4 Waarom zou een langere sleutel veiliger zijn dan een kortere sleutel?

7.5 Als geheimhouding niet door de sleutel maar door het versleutelingsalgoritme wordt verzekerd, dan wordt dit *security by obscurity* genoemd. Wat is nadeel van het gebruik van deze methode ten opzichte van het gebruik van een geheime sleutel? Heeft deze methode ook een voordeel?

7.6 Als versleutelingsalgoritme moet een one-way functie gebruikt worden.

A Leg uit waarom een inverteerbare functie niet gebruikt kan worden.

B Leg uit waarom niet elke one-way functie gebruikt kan worden.

7.7 Stel je drukt bij een website op de 'Wachtwoord vergeten' link. Vervolgens vul je jouw email adres in en je ontvangt jouw wachtwoord per email. Wat is er mis in deze situatie?

7.8 Toon aan dat bij de EXOR operatie, de sleutel zowel gebruikt kan worden voor encryptie als decryptie. Gebruik *0b101* als sleutel en *0b11101110* als data.

7.9 Wat is het grootste nadeel van het one-time-pad voorbeeld met een echt[2] willekeurige sleutel?

7.10 Waarom wordt cipher blok chaining toegepast?

7.11 Romeo wil Julia geheime boodschappen sturen. Hij wil er ook voor zorgen dat Julia kan verifiëren dat de boodschappen van hem afkomstig zijn en dat er niet mee geknoeid is. Romeo en Julia gebruiken asymmetrische cryptografie en hebben dus beide een publieke en een geheime sleutel. Met welke sleutel(s) moet Romeo zijn boodschappen encrypten en met welke sleutel(s) kan Julia deze boodschappen weer decrypten?

7.12 M.b.v. 'Diffie-Hellman key agreement' kunnen twee partijen een gelijke geheime sleutel aanmaken zonder geheime informatie uit te wisselen. Wat is het grootste nadeel van deze methode.

7.13 Vaak wordt asymmetrische encryptie gebruikt om een geheime sleutel uit te wisselen (session key) waarna symmetrische encryptie wordt gebruikt voor het uitwisselen van berichten.

A Waarom wordt niet meteen vanaf het begin symmetrische encryptie gebruikt?

B Waarom wordt niet de hele tijd asymmetrische encryptie gebruikt?

[2] Echt willekeurig in tegenstelling tot pseudo-willekeurig

7.14 Maak vraag 17.6 en 17.7 uit het boek.

7.15 Figuur 18.9 op pagina 379 van het boek, laat zien hoe een beveiligde HTTPS verbinding wordt opgezet. Kan een man-in-the-middle-aanval succesvol plaatsvinden bij dit voorbeeld? Leg uit.

7.16 Het quantum algoritme van *Shor*, is enorm snel in het factoriseren van getallen. Cryptografen maken zich hier zorgen over, waarom?

7.17 PGP (Pretty Good Privicy) kan worden gebruikt om bestanden en e-mails te encrypten en decrypten. OpenPGP is naar eigen zeggen de meest gebruikte e-mail encryptie standaard, zie https://www.openpgp.org/.

A Gebruikt PGP symmetrisch of asymmetrisch encryptie?

B Stuur een met PGP geëncrypte e-mail naar d.versluis@hr.nl of j.z.m.broeders@hr.nl met de antwoorden van de vragen 17.6 en 17.7 uit het boek. De public keys voor deze adressen zijn te vinden op de keyserver van surfnet. Wanneer je zelf ook jouw public key meestuurt, dan krijg je geëncrypte feedback op jouw antwoorden!