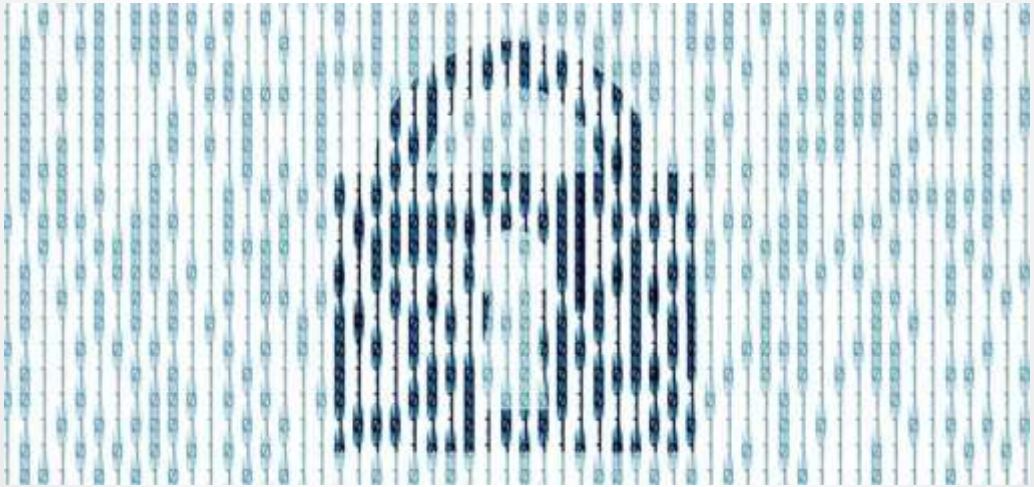
Profielwerkstuk Informatica en Wiskunde

“Is RSA-cryptografie nu veilig genoeg en wat betekent dit voor de toekomst van digitale beveiliging?”



Door Nahom Tsehaie en Jun Feng
Begeleiders: David Lans en Albert Westereenen

Wie zijn wij?

Naam: Nahom Tsehaie
17 jaar
Studie: Mechanical Engineering, TU Delft

Naam: Jun Feng
18 jaar
Studie: Electrical Engineering, TU Delft

Winnaars PWS prijs 2014

Structuur

1. Wie zijn wij?
2. Inleiding
3. Hoofdvraag en deelvragen
4. Ontwikkeling van cryptografie
5. Soorten cryptografie
6. RSA en de werking ervan
7. RSA programma in *Visual Basic*
8. Inzetbaarheid van RSA
9. Het kraken van RSA
10. De toekomst van cryptografie
11. Video
12. Conclusie

Inleiding

- Wat betekent cryptografie?
- Keuze voor cryptografie
  - Recent in het nieuws.
  - Geinteresseerd in de kennis daarachter.
  - Mooi meegenomen voor onze vervolg studies.
- Aanpak onderzoek

Hoofdvraag en deelvragen

“Is RSA-cryptografie nu veilig genoeg en wat betekent dit voor de toekomst van digitale beveiliging?”

1. “Hoe heeft cryptografie zich ontwikkeld?”
2. “Welke soorten cryptografie bestaan er?”
3. “Wat is RSA en hoe werkt RSA?”
4. “Op welke gebieden is RSA inzetbaar?”
5. “Op welke manieren is het RSA te kraken?”
6. “Wat is de toekomst van cryptografie?”

De ontwikkeling van cryptografie

I. Methode van de Spartanen

II. De Caesarmethode

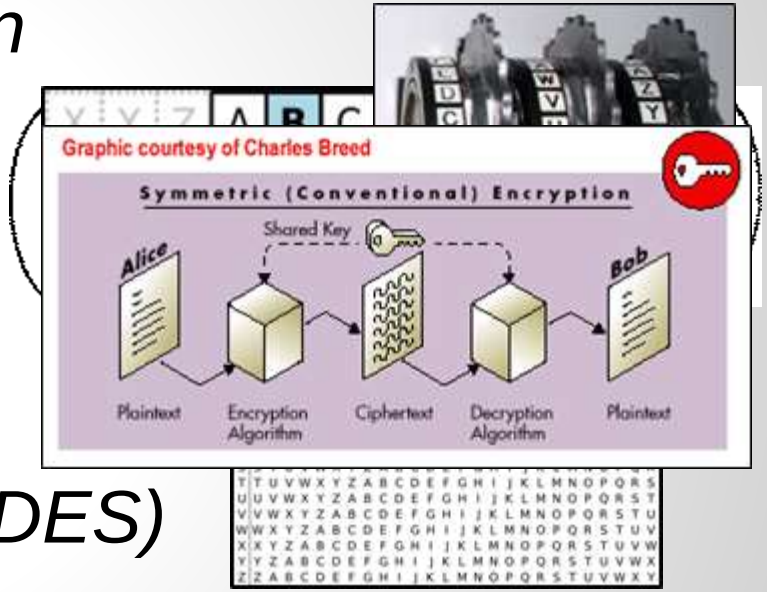
III. De techniek van Vigenère

IV. De Vernam-codering

V. Enigma-code

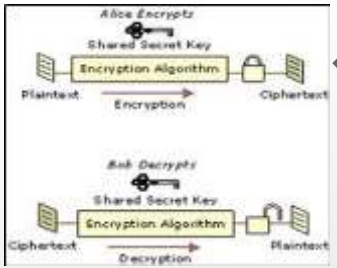
VI. Data Encryption Standard (DES)

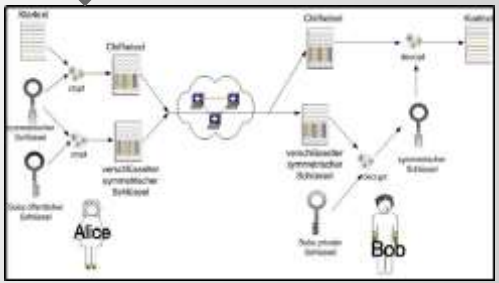
VII. RSA-Systeem



Soorten cryptografie

- Cryptografie
  - Klassieke Cryptografie
    - Substitutie-versleuteling
      - *Mono-alfabetische versleuteling*
      - *Poly-alfabetische versleuteling*
    - Transpositie-versleuteling
  - Moderne Cryptografie
    - Symmetrische Cryptografie
    - Asymmetrische Cryptografie





RSA en de werking ervan - 1

- Gevaar van onderschepping communicatie → assymmetrische cryptografie, ‘public-key cryptografie’
- Jaren ‘60: Diffie-Hellman cryptografie; nog niet perfect
- 1977 Oplossing: RSA cryptografie door **R**ivest, **S**hamir en **A**dleman

RSA en de werking ervan - 2

RSA conceptueel

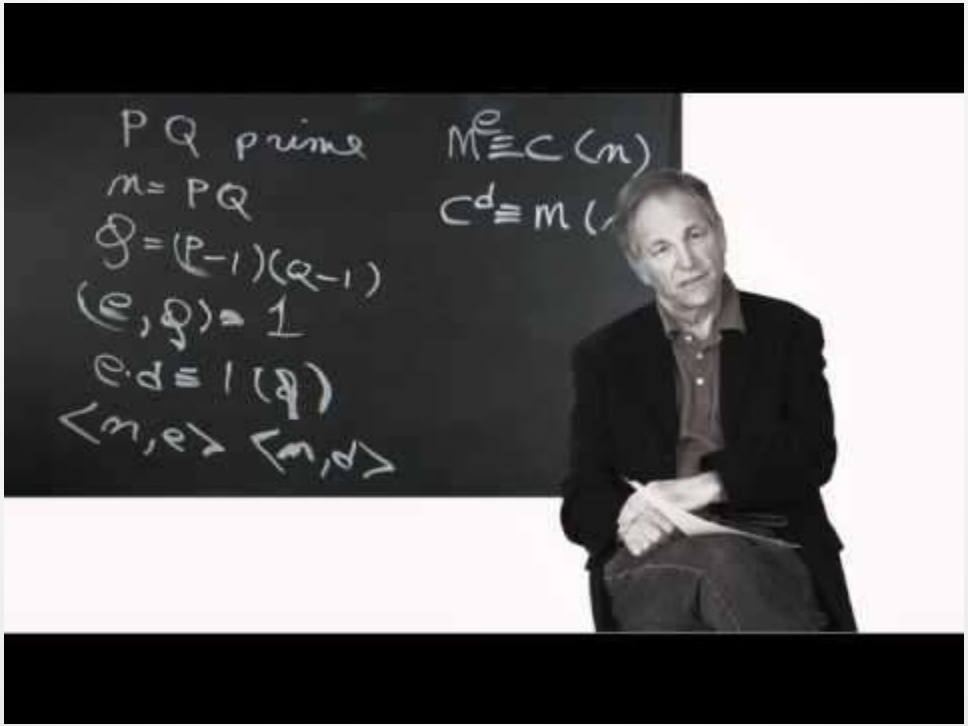
Belangrijk:
Eén-richting functie

RSA en de werking ervan - 3

- Wiskundig algoritme
- Eén-richting functies
  - Priemfactoriseren
  - Modulo rekenen
- RSA programma (voor zover dat mogelijk is) in *Visual Basic*

Video (Alternatief)

- Korte video waarbij de uitvinders van RSA het algoritme snel doorlopen [1.33]



RSA Programma in *Visual Basic*

- Gaat het programma stap voor stap door
- Laat zien hoe sleutels gecreëerd worden
- Kan versleutelen én ontsleutelen
- **Restrictie**: sommige getallen zijn té groot voor *Visual Basic*
- *Demonstratie*

Inzetbaarheid van RSA

- Lage efficiëntie van het RSA algoritme (voor nu)
- Combineren van (snelle) symmetrische en (langzame) assymmetrische cryptografie: zie mail protocollen
- Digitale certificaten (*'https://'*)
- Digitale handtekeningen: *hashwaarden*

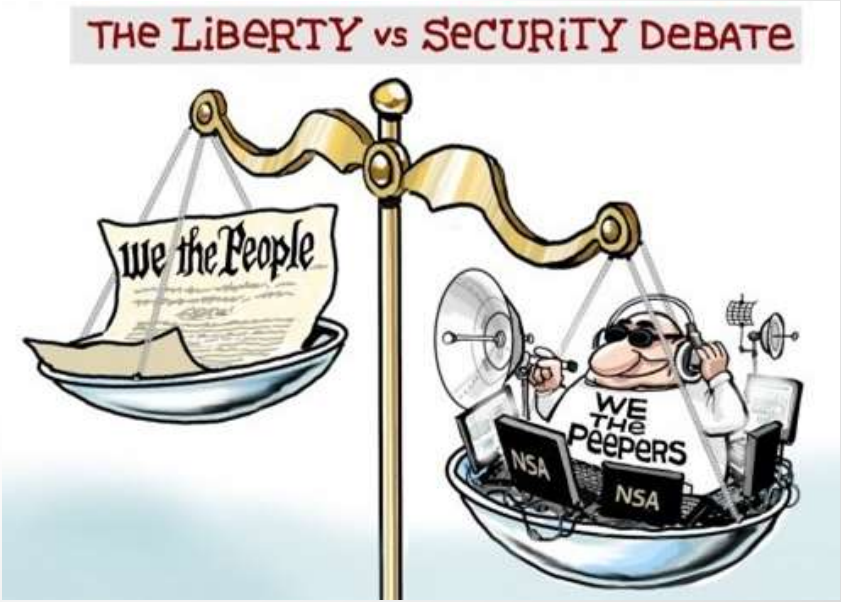
Het kraken van RSA

RSA Number	*Decimal digits*	*Binary digits*	*Cash prize offered*	*Factored on*	*Factored by*
RSA-100	100	330	$1,000 USD	April 1, 1991	Arjen K. Lenstra
RSA-576	174	576	$10,000 USD	December 3, 2003	Jens Franke, University of Bonn
RSA-640	193	640	$20,000 USD	November 2, 2005	Jens Franke, University of Bonn
RSA-704	212	704	$30,000 USD	July 2, 2012	Shi Bai, Emmanuel Thomé and Paul Zimmermann
RSA-768	232	768	$50,000 USD	December 12, 2009	Thorsten Kleinjung
RSA-896	270	896	$75,000 USD	Not Factored	/
RSA-1024	309	1024	$100,000 USD	Not Factored	/
RSA-1536	463	1536	$150,000 USD	Not Factored	/
RSA-2048	617	2048	$200,000 USD	Not Factored	/

Tabel 1 RSA Challenge numbers

De toekomst van cryptografie

- Technologische vooruitgang
- Efficiëntie verbetering
- Toenemende druk op digitale beveiliging én privacy - een zwaar dilemma (?)



Conclusie (Deelvragen) - 1

1. **“Hoe heeft cryptografie zich ontwikkeld?”**

   In de loop van de tijd is het versleutelen van berichten steeds geavanceerder geworden.

2. **“Welke soorten cryptografie bestaan er?”**

   Er bestaan twee soorten cryptografieën: Klassieke en Moderne cryptografie. De moderne cryptografie kan onderverdeeld worden in asymmetrische en symmetrische cryptografie. De klassieke cryptografie kan onderverdeeld worden in substitutieversleuteling en transpositieversleuteling.

3. **“Wat is RSA en hoe werkt RSA?”**

   RSA is een cryptografie, baanbrekend door het gebruik van asymmetrische cryptografie en eenrichtingsfuncties.

Conclusie (Deelvragen) - 2

4. **“Op welke gebieden is RSA inzetbaar?”**

   Tevens is bekend dat RSA op vele gebieden inzetbaar is, zelfs buiten het versleutelen van informatie.

5. **“Op welke manieren is het RSA te kraken?”**

   Er zijn toch verschillende manieren gevonden om RSA te kraken, hoewel geen daarvan dat in een kort tijdsbestek kunnen.

6. **“Wat is de toekomst van cryptografie?”**

   De toekomst van cryptografie is erg veel belovend, omdat de druk op de cryptologische vooruitgangen erg groot is.

Conclusie (Hoofdvraag)

“Is RSA-cryptografie nu veilig genoeg en wat betekent dit voor de toekomst van digitale beveiliging?”

RSA is op dit moment nog net veilig genoeg, zeker vergeleken met de oude cryptografie systemen die er waren voordat RSA in het leven was geroepen. Asymmetrische cryptografie is in het heden de beste techniek om te versleutelen, een techniek waar het veelgebruikte RSA onder valt. Doordat priemgetallen oneindig in aantal zijn, kan RSA altijd een stapje voor supercomputers zijn. RSA is echter niet heel efficiënt en er zijn al manieren gevonden om RSA te kraken, al zijn die manieren erg langzaam. Wel kan het zo zijn dat het versleutelen met RSA dusdanig lang en complex wordt bevonden, dat men kan overstappen naar een ander versleutelingsmethode.

De digitale beveiliging zal onder de huidige technologische snelheidsdruk steeds sneller ontwikkelen en wij verwachten dat deze steeds efficiënter zal worden, omdat RSA voor huidige standaarden nog redelijk zwaar is voor computers om informatie mee te beveiligen.

Bedankt voor uw aandacht!

Zijn er nog vragen?