Workshop encryption

Arne Timmerman, March 27th 2014

Voorpagina
Net binnen
⊞ Algemeen
Vlucht MH 370
⊞ Economie
Beurs
Sport
Tech
Achterklap
⊞ Entertainment
Opmerkelijk
Wetenschap
Gezondheid
Lifestyle
Auto
⊞ NUfoto
Datablog
Redactieblog
Weer
⊞ Verkeer
NU.nl-apps
Colofon

Gepubliceerd: 10 maart 2014 18:33
Laatste update: 10 maart 2014 20:13

Snowden wil dat techbedrijven data beter versleutelen

Technologiebedrijven moeten hun verantwoordelijkheid nemen op het gebied van dataversleuteling, vindt klokkenluider Edward Snowden.

Foto: Channel4 / AFP

"Er moet een technische reactie plaatsvinden", aldus Snowden via een livestream op het South by Southwest-festival (SxSW). De klokkenluider reageerde vanuit zijn schuilplaats in Rusland op vragen in Austin, Texas, via Google Hangouts.

Volgens Snowden kunnen techbedrijven beveiligingslagen aanbrengen waardoor het moeilijker wordt voor overheidsinstellingen om massaal data op te slaan. Dat zou bovendien sneller kunnen dan dat er nieuwe wetgeving wordt geïmplementeerd.

De oud-NSA-medewerker stelt verder dat internetgebruikers minder te vrezen hebben voor grote bedrijven dan voor overheden: "Bedrijven kunnen je data verkopen en gebruiken, maar je hebt nog altijd rechten. De overheid kan je opsluiten."

Volgens de klokkenluider, verantwoordelijk voor het lekken van een grote hoeveelheid documenten van de Amerikaanse geheime dienst NSA, zal de NSA in de meeste gevallen wel data kunnen onderscheppen wanneer het dat echt wilt. Maar het onbeperkt en massaal opslaan van onschuldige burgers kan volgens de klokkenluider worden tegengegaan door data vaker en beter te versleutelen: "Dataencryptie werkt wel degelijk".

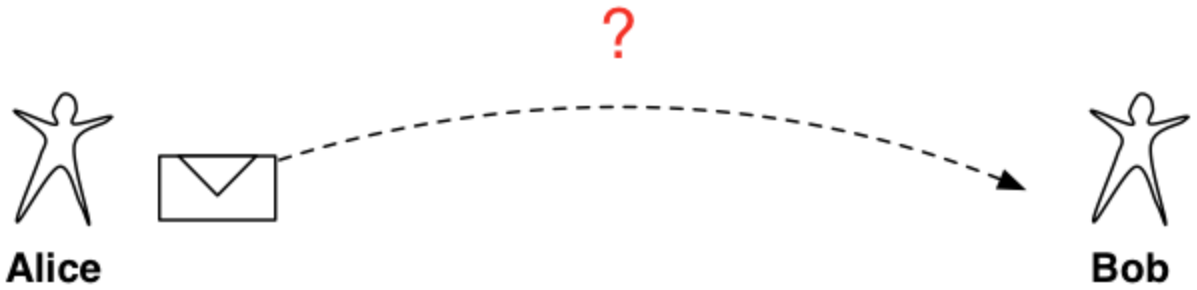
(1) Symmetric encryption

(2) Asymmetric encryption

(3) Encrypt **personal details**

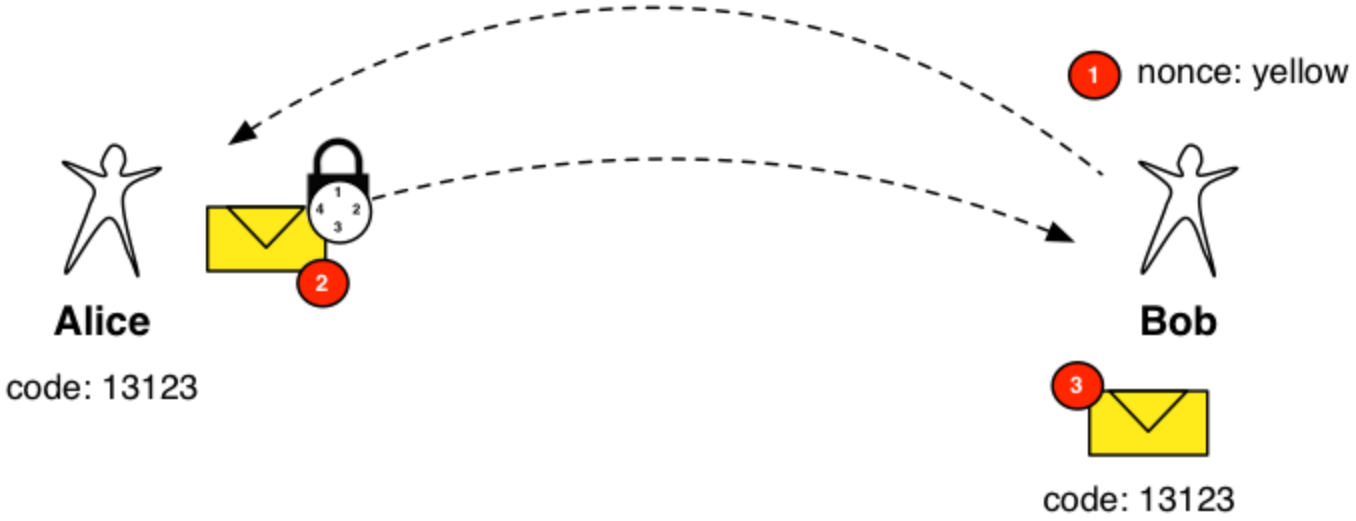
(4) Share personal details

The messaging problem



(1) **Symmetric** encryption

(1) **Symmetric** encryption - **nonce**

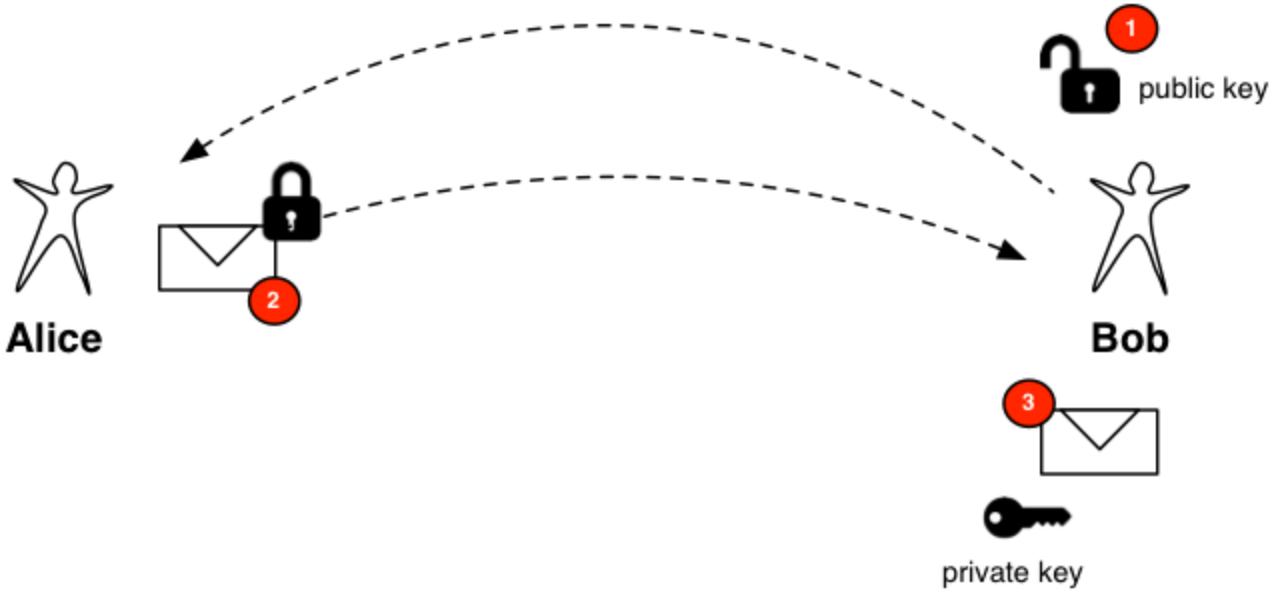


(1) **Symmetric** encryption

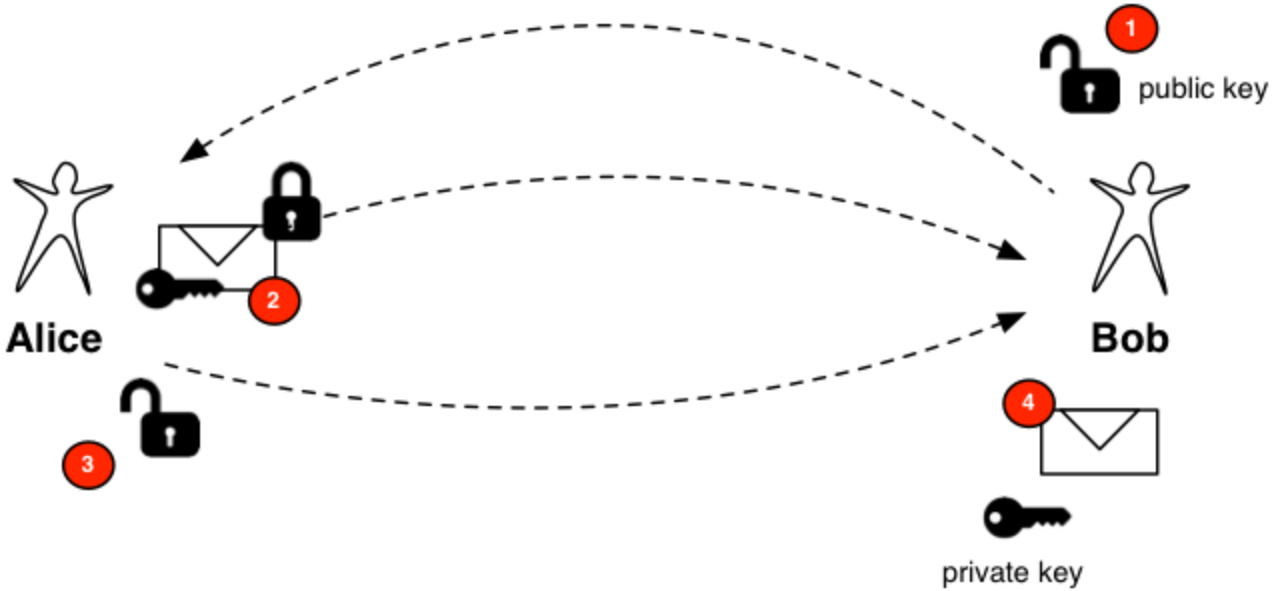
Hands-on!

- **Exercise 1**
- Open the test
- Fix TODO in *.exercise1*
  - **Java**: Symmetric.java
  - **Ruby**: symmetric.rb

(2) **Asymmetric** encryption



(2) **Asymmetric** encryption - **signing**

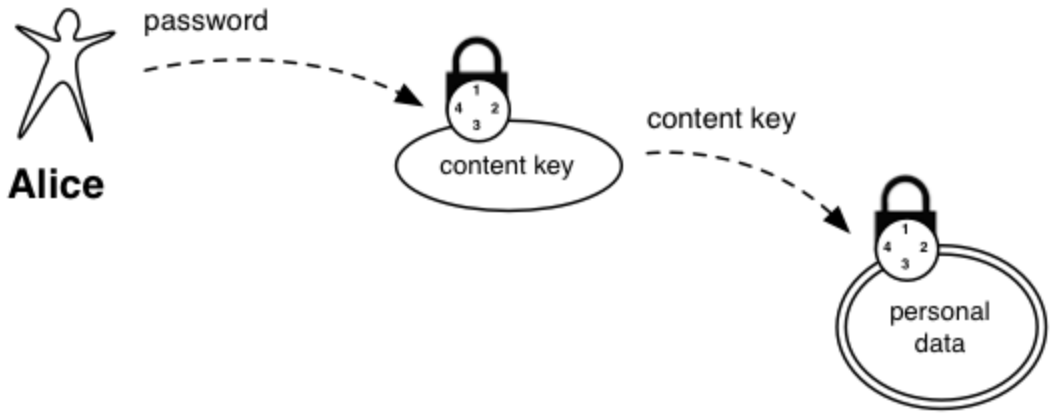


(2) **Asymmetric** encryption

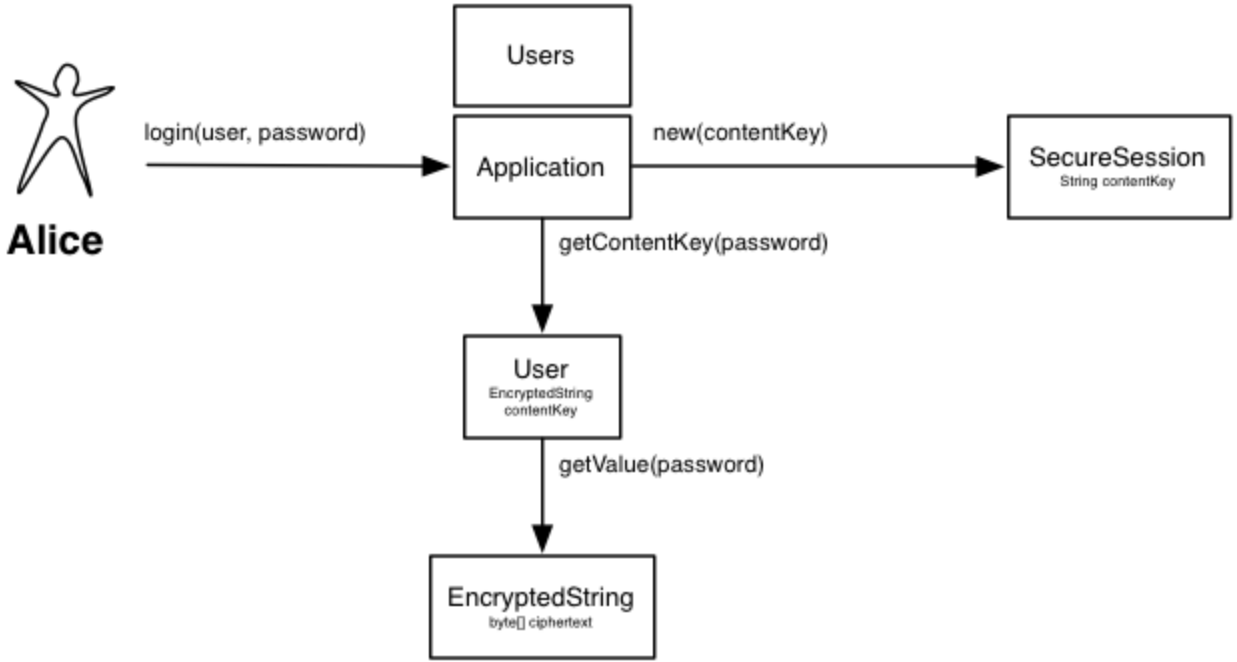
Hands-on!

- **Exercise 2**
- Open the test
- Fix TODO in *.exercise2*
  - **Java**: Asymmetric.java
  - **Ruby**: asymmetric.rb

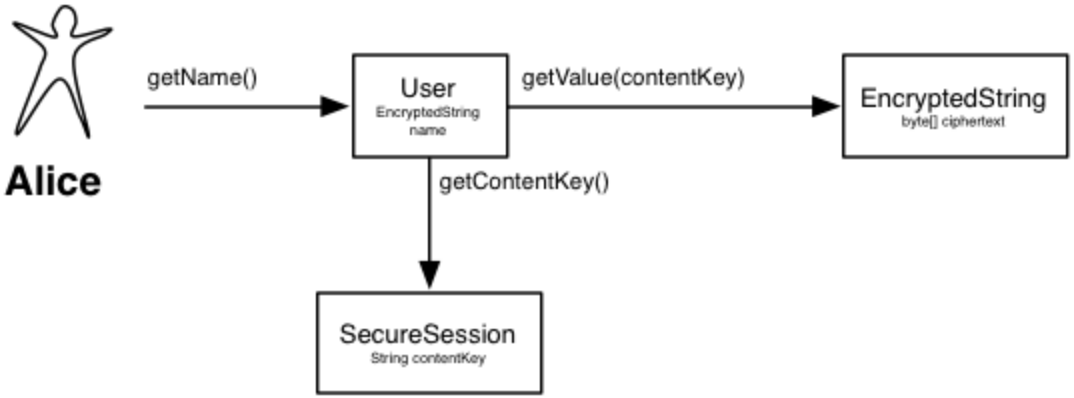
(3) Encrypt **personal details**



(3) Encrypt **personal details**



(3) Encrypt **personal details**

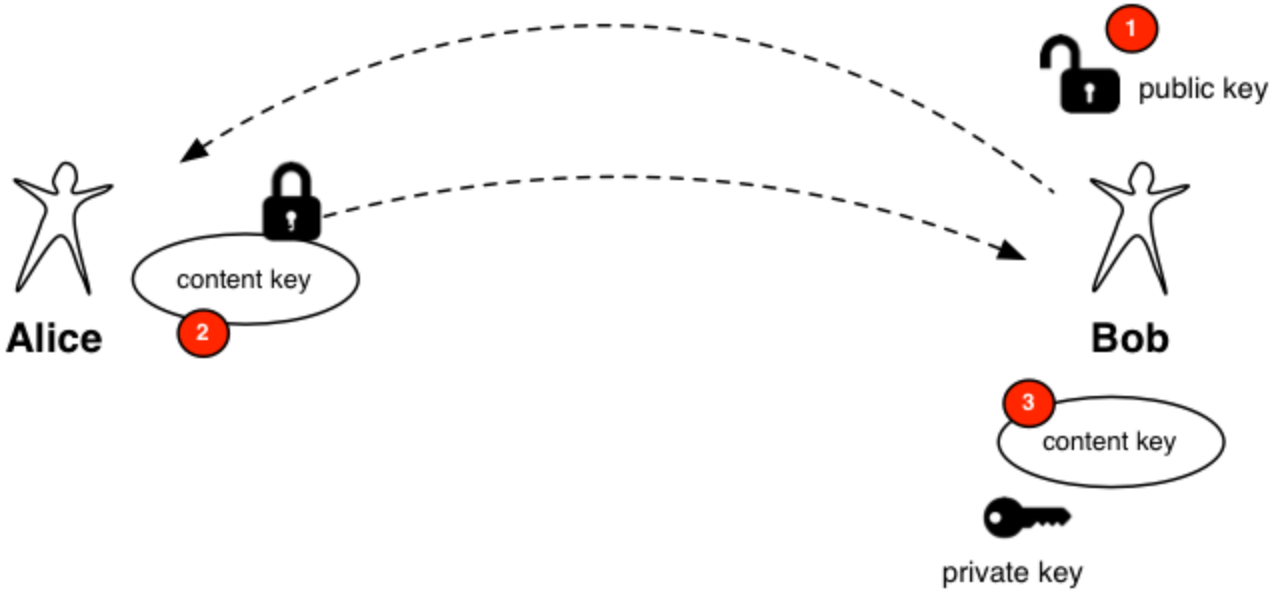


(3) Encrypt **personal details**

Hands-on!

- **Exercise 3**
- Open the test
- Fix TODO’s in *.exercise3*
  - **Java**: EncryptedString.java en User.java
  - **Ruby**: encrypted_attribute.rb en user.rb

(4) **Share** personal details



(4) **Share** personal details

Hands-on!

- **Exercise 4**
- Open the test
- Fix TODO's in *.exercise4 (and some changes in .exercise3)*
  - **Java**: AsymmetricEncryptedString.java, EncryptedPrivateKey.java and SharingUser.java
  - **Ruby**: asymmetric_encrypted_attribute.rb and sharing_user.rb