Asymetrichse encryptie

Door: Robbe van der Lee, MD2A

1) Een 4-tal functies in PHP die je kunt gebruiken voor asymmetrsiche encryptie.

1. openssl_public_encrypt();
2. openssl_private_decrypt();
3. openssl_pkey_get_details();
4. openssl_pkey_new();

2) De maximale hoeveelheid bits en bytes dat RSA kan` encrypten `.

2048

3) Gebruik je in IntelliJ een username / password combinatie voor je Github of gebruik je SSH keys.

Ik gebruik username/password.

4) Waarvoor gebruikt Github de keys als je met SSH inlogt.

Voor verificatie.

5) Wat moet er allemaal geregeld worden dat Bob ook berichten aan Alice kan sturen die versleuteld zijn.

Bob moet een public en private key hebben en Alice moet een session key hebben.

6) Wat moet er geregeld worden zodat ook Alice de berichten van Bob kan lezen.

Zie vraag 5.