TU/e Technische Universiteit Eindhoven University of Technology

Publieke en geheime sleutels

Crypto Werkplaats: Cryptografie met publieke sleutels

1. Asymmetrische cryptografie

- Bij de asymmetrische encryptie worden twee sleutels gebruikt:
- Een encryptie- en een decryptiesleutel.
- De sleutels zijn niet identiek.

2. Illustratie

- Iedeeren kan een doos met een hangslot op slot doen,
- Maar alleen degene die de sleutel heeft, kan het slot weer openen.

3. Anita

- Anita wil dat iedereen haar een geheim bericht kan zenden zonder dat iemand het bericht kan afluisteren.
- Anita maakt twee sleutels die bij elkaar horen.

4. Twee sleutels

- De publieke sleutel wordt gebruikt om een bericht te versleutelen. Hij kan het bericht niet ontsleutelen.
- De geheime sleutel wordt gebruikt om een bericht te ontsleutelen.

5. Sleutel management

- Anita maakt de publieke sleutel bekend, zodat iedereen deze sleutel kan gebruiken.
- Anita houdt de geheime sleutel geheim en bewaart hem zorgvuldig.

6. Benne

- Benne wil Anita een bericht sturen.
- Hij zoekt Anita's sleutel op (b.v. op een keyserver).
- Hij versleutelt het bericht met met behulp van de publieke sleutel.
- Alleen Anita kan de cijfertekst weer ontsleutelen omdat ze de enige is die de geheime sleutel kent.

7. Christiane

- Voorbeeld: Christiane's publieke sleutel is een 2048-bit RSA sleutel.


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.7 (MingW32)

mQENBEbMpFQBCACyO8RaYCRoQNUYZGx1AdCOhWhIuqSbrAmx9HOc+5ZFRv/Tf3cX
M7IqBSwAyo5dOo7EGVRNCyh8qnF/YeyulTz9Kcat4BfMCYGILw+ngwQVpSs+sprP
JA+FilfGVvMLQMKNoSnMCQc7B5UF0wtwWyZ7OPlICcs9OzExIoyI/7gDh8wHoZkQ
mC96OQZZLqL7Yxitd/EmKYQK2josCRxoMw+wnMJ7SC2oWLOOftN4LRrp1Q5nCnic
5GUmvH8vZhNIQoAEmmuWKgMiP8TC2nm6+/uofyFVSHpkRVxuVfAkkJVk2XrIFPVZ
nMB/8rkueXcflXlQpCln+lf96KmnQv9eksELABEBAAG0L0NocmlzdGlhbmUgUGV0
ZXJzIDxjaHJpc3RpYW5lLnBldGVyc0BnbWFpbC5jb20+iQE8BBMBAgAmBQJGzKRU
AhsjBQkJZgGABgsJCAcDAgQVAggDBBYCAwECHgECF4AACgkQKaf+lZlk07ErnggA
np83E80m6jRwrZqbajxrE4nlOBIFg4vfPOekwL+jkG5XvE2y54GTAXc/Mywb4BkQ
jsUxYqmtqBGyPMJREy239z9fZRLLGh3l++/QgJ5GznQpBMzmgJKmZGzLtN8WhHkj
wBA7m7SZnwvpKTDQwNCLCdGFm5/PHvWjBVlm4EWuIqYZySCwx3jLaXhD/XixfZyL
Q7scDHGZ6NVgDhmj7/9vmsc+Ekf46aLe51dSSy94A8aPCVIRXGZFXTWX46k/vsv2
OOC7GvVjd6HsgcVMxD72o9ky5ccpKOvmwIrmV/Gg3STyTAu9ZToV6hglYxXoHX+3
NFnfv8Bf7Gavsol LtoEZQ7QlQ2hyaXN0aWFuZSBQZXRlcnMgPGMucC5wZXRlcnNA
dHVlLm5sPokBPAQTAQIAJgUCRsykvAIbIwUJCWYBgAYLCQgHAwIEFQIIAwQWAgMB
Ah4BAheAAAoJECmn/pWdZNOxQmoIAIH+ZPDS5REq8vJPxb7d/x3fxE+AkclOKeRH
xdc9m78mSp0xkJTvL2VGI0tSGElMKto6hrEaW+3JJEdyD30Qrz7L1X5JrJC2pNDr
KPM9ikJ2tqvsRzaBBkLpjmbHw7slKsUGQsOHPZgVVqdGgE9Wz8g+MduYQiTgsyjb
m8DtYeUOgOoC43NOLu6p5dN3krPWaixXzXhaJrLIfpOgMmOGzlsSQJGasvItLwEg
/Nq2uZrnAswHctlOpXsaMr5IAO/fkb5Z3+q4wegR57SKIQ/RIvvzwLs5xPiiZHBv
oBI+jJKBlTl+xx9fkWx4d+UbMKWmK9qCSyKelxP/ulknrv3gDna5AQOERsykVAEI
AOLbYjcRDp21FwBMKtk/5vjkTXwH74wdQtVtR9KghRPhlN8SbEpFrwY1s28LMnxt
+GBAQydS7BrI4iY8VtcWSh+/5ihDxBdOl5sb+O4uYqUNWQ77Hwo9YdVVvdGXUSC/
+rMgCmDWpOOSAXOijh587zZFqaSkg8OGLa5B7xXCNoSY92aLtJ5Kks+XgtfHyxqX
ijtu3h2ZRn/bWWvpxyBb+KLUl8cjt/QuMoq99ymxUi4P4MT6xMKicG6fOMkQzKJK
Fctl+WHU6pom4YQKV6lwK6NHxY6YopjX+puCySUBLPxP89cXgu2sugU4rE6yYJjO
lP3t7swweDPaKHexXBUwBr8AEQEAAYkBJQQYAQIADwUCRsykVAIbDAUJCWYBgAAK
CRApp/6VnWTTsYgoCACE/AJ2EWlwQHrQmWRnGVYxDKiZdb0LSZ/4Dj+xjKKWyIhv
7C5s5Bvt3QGbUC4ui/SW2ih5kNIasTZZ3R5Zeq3sb1g1tXUBBpUPfYO7CLnd9Qk8
fmm6XN5ulkiFjuI85xL83yUZazw0TYSITRlYQXhyFaSKtedxJJbVOreWCilvmOFh
tczAo9kdzCsajMdb8L0nm+AjfpccETFNrz9ZebF5JCZYRG7It2UyOs6JtoC8HC+G
pacMNeHjh820koY1KZaEaqPGPFIaHYviBkSUkLQtZ4H78KvSf+D888JwzQZawN4s
ofRjQv3R2CBLCmt4TUmbeuzjiOMBVaLYnHxxdsI1
=stPR
-----END PGP PUBLIC KEY BLOCK-----
```


8. Gebruik

- Deze sleutel is te vinden op haar website `chris-tianepeters.wordpress.com/abou` of op een keyserver.
- Om Christiane een versleutelde email te sturen gebruik je de publieke sleutel samen met je email programma zoals *Outlook* of *Thunderbird*.

9. Laat je kunsten zien

- Veelgebruikte systemen zoals RSA-2048 zijn uitgebreid bestudeerd en worden als veilig beschouwd.
- Wij hebben hier twee systemen die met de hand uitvoerbaar zijn.
- Je kunt hiermee je kunsten als cryptograaf of codebreker laten zien.