

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.

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.

7. Christiane

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

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

mQENBEBMpfQBACACy08RaYCRoQNUY2Gx1AdC0HWhIuqSbrAmx9H0c+5ZFRv/Tf3cX
M7IqBSWayo5d0o7EGVRNcyh8qnF/YeyuLTz9Kcat4BfMcyGLw+ngvQvpSs+sprP
JA+F11TGVVMLQMKNoSnMCQz7B5UF0wtWwyZ70PLiCcs90zExLoyI/7gDh8WHzKQ
mC960QZLqL7Yx1td/EnKYQK2jesCRxoMw+wnMJ7SC2oWLO0fTnALRrpIQ5nGh1c
5G0uvH8vZHN0oAEmuWkgMlP8Tc2n6+uoFyF9SHpkRvuVfAkk3Vx2XTPVZ
nHB/8rkueXcfYL1OpClnv1f9ekmQv9ekSLAEB8AA60L0hccmLdG1hbnUgUGV0
ZXJzIDkjaHJpc3RyYW51LnBldGVyc0BnbWVpbC5jb20+IQE88BMBAgAwBQJGzKRu
AhsjBQKJ2gGABgsJCACDAgQVAggDBBYCAwECHECF4AACgKQka+LZ1K07ErnngA
np83E8cmGjRwrZqbaJxrE4nLOBIFg4vfP0ekwL+jk05XvE2y54GTAXc/Mywb4BkQ
jsUxYqmtqB6yPMJREY239z9fZRLGh3l++/0qJ5GznQpBMZmgJ3KZGZltN8WHKj
wBA7m75ZnvpqKTDQwNCLCdGfM5/PHWjBVLm4BwuIqY2ySCw3jLaXhd/Xi.xfZyL
Q7scDHGZGNvgDhmj7/9vmsc+EKf46aLeS1dSSy94A8aPCVIRXGZFTWK46k/vsv2
00C7GvJgdHsgcVMx07209ky5ccpK0vmmVrnV/Gg3StyTAu9ZToV6hGLyxXoHX+3
NFnfv8Bf7Gavso1LtoEZQ7QlQ2hyaXN0aWUzSBQZXRlcnMgPGMucC5wZXRlc3NA
dHVlLn5sPobBPAQTAQIAJgUCRsykVAIbIwJCWY9gAYLC0gHawIEFQIIAwQMAgMB
Ah4BAheAAAgJECm/pwU2NDvQmoIAIHAZP85REa8v3Pb7d/x3fxs+Akcl0keRH
x0c9m78mSp0skJTVL2VG10TSGLWkto6HrE8W+3JJE5yD30Qr27L1X53rJC2pNDr
KPM9ikJ2tqvsRzaBBkLp1nbHw7sLksUGQs9HPZgVVqdGgE9Wz8g+MduYQitGsyjb
m80TYeU0g0c43NOLu6p5dNgrfWai.xXzXhaJrLIfp0gMm0G21sSQJGasvITLwEg
/Nq2uZrnAsvHct1OpXsaMrSIAO/fkb5Z3+q4wegR57SKIQ/RtVvzwLs5xPiizHBv
oBt+jJKBLTl+xx9fkWx4d+U6MKWk9qCSyKlXp/u1knrv3gDna5AQOERSykVAEI
AOLbYjcRdp21FwBMtk/SvjKTXwH74wdQTVtR9KghRPHN8SbEpFrvY1s2BLMnxT
+GBAQd57Bri4iY8VtcWSh+/5ihDxBd015sb+04YqUNWQ77hwo9YdVVvdGXUSC/
+rMgCmDWP005AX0iJh587zZFqaSk980GLaSB7xXCNoSY92aL1J5Kk++XgtfHyxqX
iJtu3h2ZFn/bWwpxyBb+KLUL18cjt/QuMoa99ymxL14P4MT6xMKicG6fDMKQzKJK
FctL+HWU6p0m4YQKV6LwGmHxY6YopjK4pUCYSUBLPxP89Ckgu28ugU4re9Y1jD
1P3t7swweDPaKHeX8LwBr99GEALYV9kQYAAIDwUCRsykVAIbIwJCWY9gAYLC0gH
aAwCRApp/6VnMTTSYgcACE/AJ2EWLwQHrQmWnGYyDKiZdb0LSZ/4D++xjKQWjThv
7C5s5B73qdbUC4ui/SW2ih5kNIastZZ3R5Ze9q3sb1q1tXUB8pUPfY07CLnd9Qk8
fmm6XNSUlk1FjUI85L83yUZazwOTYSITRIYQXhyFaSKtedxJ3bV0rWcL1vn0FH
tczAo9kdzCsaJmDb8L0nn+AjjfpcctETFRz9ZebF5JCZYRG7I12Uy0s6jtoC8HCg
pacMNeHjh820koY1KZaEaQPGPFIaHyv1BkSukLQtZ4H78kvSf+D888JvzQZawN4s
oFRjQv3RZCBLCnt4TUmbeuzji0MBVaLynHxxdsII
=sTPR
-----END PGP PUBLIC KEY BLOCK-----
```

2. Illustratie

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

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.

8. Gebruik

- Deze sleutel is te vinden op haar website www.win.tue.nl/~cpeters/ 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*.

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.

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.

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.