

# PGP/GPG

- PGP créé par Ph. Zimmermann
- Aujourd'hui :
  - PGP (Pretty Good Privacy) : commercial
  - GPG (GnuPG) : version libre (licence GPL)
- Combine techniques symétriques et asymétriques
- Permet de chiffrer et signer numériquement
- Bonne harmonisation avec les logiciels d'emails

# PGP/GPG

- Génération des clés
  - Aléas obtenus avec l'aide de l'utilisateur
  - Création de deux paires de clés pour chiffrer et pour signer numériquement
  - Clés secrètes sauvegardées sur le disque dur, dans un keyring, chiffrées grâce à une « passphrase »
  - Clés publiques insérées dans un certificat
  - Le certificat reprend aussi les algorithmes associés aux clés, les cryptopériodes des clés ainsi que des informations relatives au propriétaire de ces clés

# PGP/GPG

- Certificat « autosigné »
- Certificat peut être signé par des personnes tierces
- Confiance :
  - soit via la chaîne de confiance
  - soit via fingerprint du certificat

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v1.2.1 (GNU/Linux)

mQGIBD6QUQURBACqY8S00k06+xaC+bB0cPLNAutWQz8L/Dka0Fc03LoiH31cZVt8  
BntHCoKoNqE0KjtHtaxySjIAUJst9aU9MacgxF3shMivM/dPNtK9uiXWnNgB9/2H  
LfaC9+611V07Z1Htf7+0cNwLgHkfsBLF3d0nkdeZhWXpoYa5P+UcsZRvpwCg5GPF  
vdDGeD1AwwSVzygpHMbPIb8D/jbQ2ia7lCnvmFtSx6MpvniXcB0b+Z/6Jyz4qCjQ  
ZQKaHD0rUnAoXIHkVdVj20HJGsyhZio1KkIU/N1Dp6n4m0YR1xTuWaqG617NRqK  
WWQYZkhyYg44EP+xtkVckXu1REsFbG4bUPvB90y3ChkFhwP8pv7Jo7mn0uCB3Lz0  
Hk7PBAC0+4dW3dKT2ntIURuzQ8FyKAZGsQy44v4Qu9MF922WDvDJSSM7Hzktzcqn  
XZqt6hAkt8n/61AKKfVTeWo6ks/ofl6hU06cB3YjWy+zCIZ8L+iKltans4SD3j1C  
Dm1bS0ewQCU73Xwof/H+lPvil1w3WPni/TEv7hvxSGfwTLR6bQrT2xpdmllicBN  
YXJrb3dpdGNoIDxvbGl2aWVyQG1hcmtvd2l0Y2gubmV0PohZBBMRAGAZBQI+kFEF  
BAShAwIDFQIDAXYCAQIEAQIXgAAKCRDW9BbG2gEkkjGaAKCeudY/L6sL+VTN4djM  
60S/PR0IPgCaAx0f/ULXMtr2VmHhjmK+5yPMPMa5AQ0EPpBRBhAEAIuTk+LLNYhz  
72q/ZspvmjK+cCcKAZ2Iff97jliF/TK89Q0R0GuBleZtD44r0KMek+GbtFBUqZ2V  
FdkurIGCc5amd6ewiw7A7+v6KqKRU2yK4+k+ZsWqUAYJTh6ZY9ivdYauEnQba1uA  
VdpZHsMao0VqvjlHux6o5L4mXNSuXmZ3AAMFA/9H6Vjk9pQt/ZdosFQuZTXbTCvd  
3uLY87PeDYHqeo4sU+5f0lu1XJ8L+9KZu97TTE/vwHfafa1v/Dg5K9PFaCa7BHma  
gHYFvf7G0SyyBWpps0HNwIDPxz34StTPTW6oj9SadCiZsyk0MLd08jbR6iinriZJ  
Ytqo1zEJ8MjvqbTFHIhGBBgRAGBQI+kFEGAAoJENb0FsbaASSS0qUAoNaPCzaK  
xxGxzaSm7n0jgXKLweSEAJ90tuXcKUJ65ut6JKZCTQVCmYtCQw==  
=UqpM

-----END PGP PUBLIC KEY BLOCK-----

# PGP/GPG

- Chiffrement :
  - compresse le message
  - crée aléatoirement une clé de session
  - chiffre le message compressé avec la clé de session
  - chiffre la clé de session avec la clé publique du destinataire
  - envoie au destinataire les deux informations chiffrées

```
> gpg --fingerprint roggeman
```

```
pub 1024D/E59B82F7 2004-08-31 Yves Roggeman <yves.roggeman@ulb.ac.be>  
Empreinte de la clé = E2BA BF19 5482 6D86 9639 9B5D F46C AFB1 E59B 82F7  
sub 2048g/B230E385 2004-08-31
```

```
> gpg -a -r roggeman -encrypt message.txt
```

```
-----BEGIN PGP MESSAGE-----
```

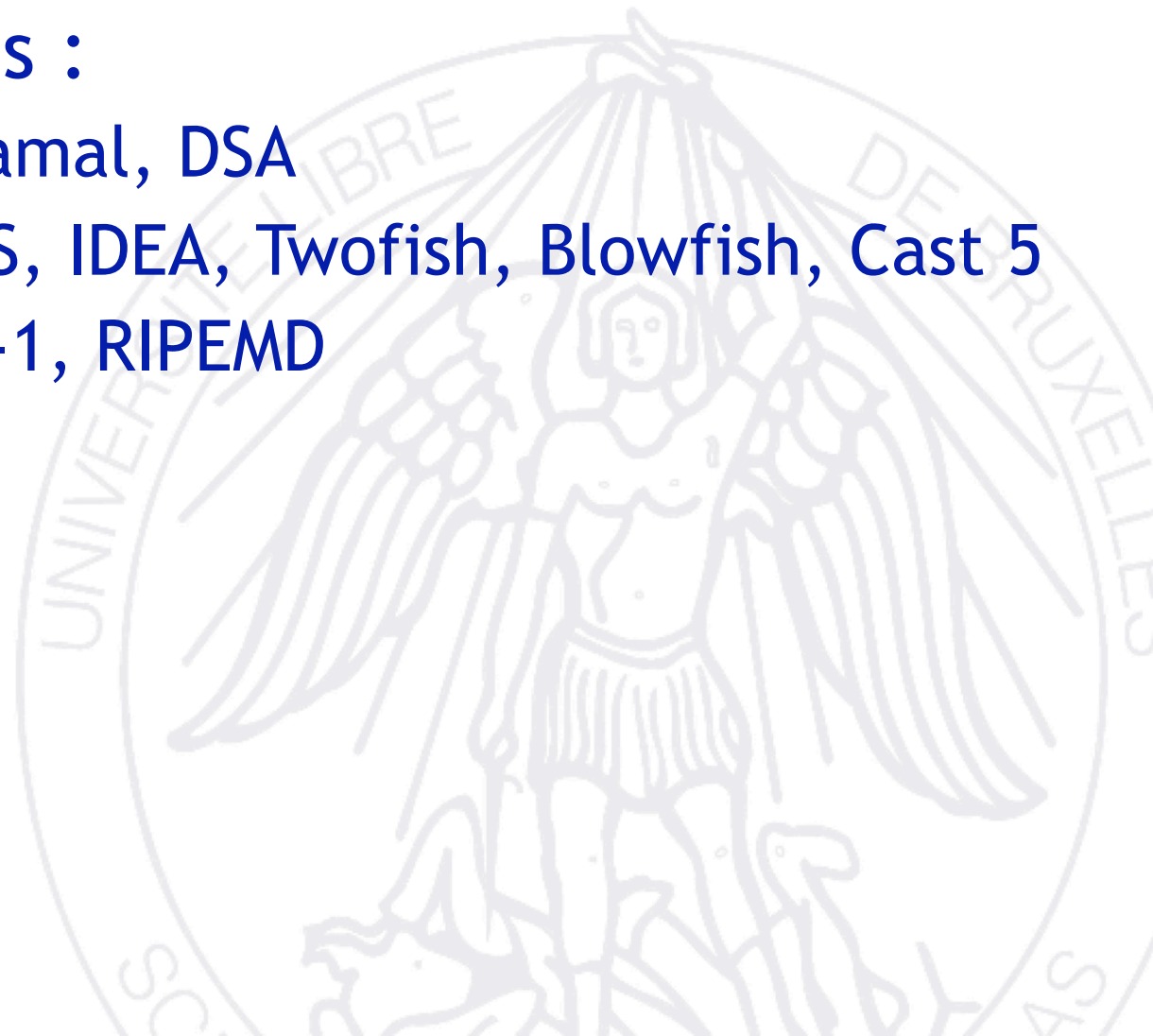
```
Version: GnuPG v1.2.4 (GNU/Linux)
```

```
hQIOAy875Z0yM00FEAgA6P0q8GNKRQ0E9fjwqgEedgc7LCelCjA0RG+9gKMZXWdN  
mbjWni1tv9c0H53YM+QVguLzE4D0u7pEifI7Nk1bbgLSVgpBayNdoSnshaEmHZh5  
ZE3EJdgDxJWCJNtewJS0EZHK97ywdi+3Ev00YQdGrTLL2mJlWEh07F748DhX7BNn  
TkQRP+d//FM+8sfoQ+ss3LXXu3kLLtPvBkQ1GcPtOo1rdfFcRZl+yWffiTJYmi4+  
RdZG995MgUi481tZKwxNb/bhpuSUPJ0QfYR0jbCambTQ3P5z6DPrzrSB8G+sL9Kz  
gIeYgPbQt0fd/F9pQbDT0mjz0R2n053CEKF3zi+D8gf+PfwIHbvyXWmH5c+1Jzur  
60XuXGTZnTnG0pggnAlSkf8HE6ER+05J7GnRIVT3n1Mzl/g/YyroMEv9/raZ9Wgj  
aIKUE2rFM3LA0CcJrfsTS2f0jWtwJLXZRSLs+xbuBTatuuB0/MxTfPNhTzYDIshX  
9j7GsmBhNzgZEHEWH6YT9TMhj0ac/XgizqcmwdGAt8Vzc4fnhaYBG/tX0bjVn9ih  
YTN74Kw2B1BNBoPBsY0+PMGGWyyGddEk8CQx/N0C8Y6QZvw7prcIEW6wlpxJ/FUX  
m8oWwukLzLxl80khWwpBwMBDAZKA6/sY+EiKGu+mz8Hs9W4GaU8hZ5kJGQLK0PwC  
PtJaAQB9N+8Vuta1JSdx7bEqWI00AxeY4Q9eCCIJKS/bENuNB9x4cHHwSisP6gwP  
/6+lyknx2NVXeqKTZ7p53qk19g5kDUQD9CQWeFWqbx8ADazriZc81jk/P+J2  
=6aGz
```

```
-----END PGP MESSAGE-----
```

# PGP/GPG

- Algorithmes :
  - RSA, El Gamal, DSA
  - 3-DES, AES, IDEA, Twofish, Blowfish, Cast 5
  - MD5, SHA-1, RIPEMD
  - Zip



# SSL/TLS

- SSL (Secure Socket Layer) : Netscape
- TLS (Transport Layer Security) : IETF
- Assure l'identification, la confidentialité et l'intégrité
- 4 sous-protocoles : handshake, change cipher spec, alert et record
- Modification de la pile TCP/IP
- Modèle client/serveur

# SSL/TLS

- Handshake :
  - Initie une session SSL/TLS
  - Identification (mutuelle) du client et du serveur
    - Utilisation de certificat X509
  - Sélection des algorithmes utilisés
    - Liste d'algorithmes proposés par le client, sélection des algorithmes par le serveur parmi ceux de la liste
  - Client envoie confidentiellement une clé maître au serveur
  - Client et serveur déduisent les clés de cette session SSL/TLS depuis la clé maître

# SSL/TLS

- Record :
  - Découpe du message à transmettre en blocs
  - Compression éventuelle des blocs
  - Calcul du MAC de chaque bloc
  - Chiffrement du bloc et de son MAC
  - Transmission de l'information chiffrée à la couche TCP

IDEA, DES, 3-DES, AES, RC2, RC4, Fortezza, MD5, SHA-1

# SSL/TLS

- Alert :
  - Génère des messages d'alerte
  - Warning
    - Exemple : mauvais certificat
  - Erreur fatale
    - Clot la session SSL/TLS
    - Exemple : mauvais MAC

# IPsec

- Protocole modifiant la couche IP
- Assure la confidentialité et l'intégrité des paquets IP
- Transparent pour les utilisateurs
- 4 sous-protocoles : AH, ESP, IPcomp, IKE

# IPsec

- AH (Authentication Header) :
  - Protection anti-rejeux (numéro de séquence)
  - MAC sur le datagramme
- ESP (Encapsulating Security Payload) :
  - Datagramme chiffré
  - Protection anti-rejeux (numéro de séquence)
  - MAC sur le datagramme

# IPsec

- IPcomp : compression du datagramme
- IKE : protocole d'échange des clés nécessaires aux MACs et aux chiffrements

DES, 3-DES, RC5, IDEA, CAST, Blowfish,  
AES, HMAC, MD5, SHA-1,

# IPsec

## Mode transport

- Datagramme IPsec transporté tel quel par le réseau
- Nécessite des équipements intermédiaires adaptés

## Mode tunnel

- Datagramme IPsec encapsulé dans un datagramme IP classique
- Réseau privé virtuel (VPN)

# Réseaux sans fils

- **Wifi**
  - Wireless fidelity
  - IEEE 802.11
    - 802.11b : débit 11Mbps, 300 mètres, 3 canaux radio
    - 802.11g : débit 54Mbps, compatible 802.11b
    - WEP : chiffrement faible
    - WPA : chiffrement amélioré (TKIP)
    - Filtrage adresse MAC
    - Futur : 802.11i (AES) : nécessite nouveau matériel
- **Wimax : IEEE 802.16, 70Mbps, 50 kilomètres**