

Cryptographie et sécurité
IFT-606

Devoir 1 - Cryptographie et attaques

Amandine Fouillet - 14 130 638
Frank Chassing - 14 153 710

18 février 2015

Table des matières

1	Wi-Fi	4
1.1	Fonctionnement des trois algorithmes de chiffrement	4
1.2	Points faibles et attaques possibles des trois algorithmes de chiffrement	4
1.3	Aircrack-ng	4
2	Chiffrement et signature	4
2.1	Génération d'une paire de clé RSA	4
2.2	Création d'un fichier contenant la partie publique de la clé RSA	4
2.3	Chiffrement de la partie privée générée	4
2.4	Chiffrement d'un message	4
2.5	Déchiffrement d'un message	4
2.6	Signature du fichier	4
3	Attaque décortiquée	4

Table des figures

1	Génération de la paire	4
2	Fichier obtenu	4

1 Wi-Fi

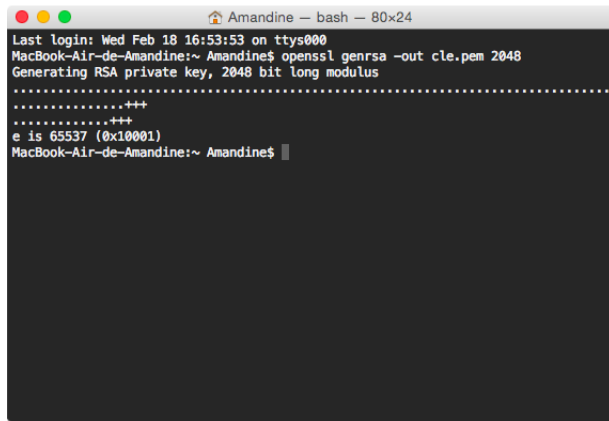
1.1 Fonctionnement des trois algorithmes de chiffrement

1.2 Points faibles et attaques possibles des trois algorithmes de chiffrement

1.3 Aircrack-ng

2 Chiffrement et signature

2.1 Génération d'une paire de clé RSA



```
Amandine — bash — 80x24
Last login: Wed Feb 18 16:53:53 on ttys000
MacBook-Air-de-Amandine:~ Amandine$ openssl genrsa -out cle.pem 2048
Generating RSA private key, 2048 bit long modulus
.....+++++
.....++
e is 65537 (0x10001)
MacBook-Air-de-Amandine:~ Amandine$
```

FIGURE 1 – Génération de la paire



```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvcvxi3zrwoBt+VCPtkufy682ZMVHg3cuZaFrFWL08efBSM
9HksaKaMjWwPBRAsyb0gWNLj+VHfVvU7r+7HmP1taBjNL30c8BZcoIKPcy
ePpQbJu30AJWKYLAWNHNAY09seZ4JBRlKb1CktUTsHsCo189bfg5RM3C9C60vY
Py8KjXbo0D7A0oP9lsQEDokj2XsneK/x4EPsedl014ZfL19RoABTxaQ+7agq/C2Q
FidhHalqcskZ63P4+oghCeDj3McMkj8Gx0CVMcncUXf/CzfhHxBS7aPL9fkrR8
eAsI/f49x2RT2LYqvlb/9nIYKQ06McbL6LDQIDAQABAOIBAHsYp0KwYZCYEQ0r
blqiH7Mze6+VT2+7DFFmSLED2paGzEWXtEAb2uKh0WH8o6/kk98E3gg20965gUa
dRxF1z8Q7MT01XNVL1W5leZVz50sjaU58K1kxplPLTF+rBdLozJVGfInqvLSphN
k8BfxoZgaFZJc2INRb+ZzE1g+SZ5Qz3vp187VVYnD3MH17Dgu8ALN17BPuN3nTT
C4xCV67QjIH/PNSdtb61nPSFPvhtIYdsdtRG/f1oYtta4n03gZSjPjg3gU+APgvB0
r2g5cwhmN+z0VYqNRes0kidzIiat/kPpcsnNZTK6npu1uoewGjkcUs3ykfjNw1vo
D06ThPECgYEA4MB3PC/QW7f61A18Rs8UJ6S9JecY0Z3nP9PzB403Kumt0MZyWgQ
4WJePAF4ozjBRGTHVQGU+eKdbJCPjVKf0cfLYJd1/qPYa09Q30BEVCKC+pikZ
6Us3bW3G9pf0vK243vHWB81lx0sUz8Q8jZ+vvloT5dpFuRslSTUS1RRcCgYEA2DB1
aCrfsuZ/uhbLJr1rg+2ULwxXlRFDUXu7Q1u01HV+gRFA9zdsVHKyc68HUR0KMorw
719KYj+ad+fTDzPJMFLf6d8xeV7R37yy0sMJP12cTTC+gtrYrnTR1JInDyvvuY/Y
J6K0x4TBVcYGRngWU8rSDRy3j/FEyn5TMs2D3sCgYEAH2pxYZImWucYypFH07m
X/p9s+k73cAy7vICRYRo1KYWLEGFIE5dpphChpy9Im5NkdCduoia9jv4MpkLYvr
RLtdt2LnMkBJLmoaB06FXKT/icvgxXM70KEKW/BpR22dxYRqIqlg7poQR31dFM2
4fN09er97bJ1eNuL9MMrf2cCgYEA6vL/Jc4yfwLyHRNyhSnnByHTwa3wIt1TA+Msh
eEn7T4j1bE+4x1hFwyv0/mMQHw1KWjGn99UAVKN5GtVfVgSdnBampjuT43uhKz6v
lB0SL8Lscx5u2Vdt1Wsv/4021c4yJFwoOKTScHp0A5m1M3MKljzswN0HG9CTRwxj
v/t3rQKBG56QKLYPAXBYI7ucnY0rmXD28mRipvkAbcPwLkRMy29KV6Z481IRfNP
3jV9VjToZx+H15CJLfncm5D05q/adAJPI5s0pPf+oNKHvdPjv3ZiGj1345/Lv1KF
KfjUK+e2WHI799G96awPoyFL10ZgI/Q6lq1FD+M85lWqyN94j1Yg
-----END RSA PRIVATE KEY-----
```

FIGURE 2 – Fichier obtenu

2.2 Création d'un fichier contenant la partie publique de la clé RSA

2.3 Chiffrement de la partie privée générée

2.4 Chiffrement d'un message

2.5 Déchiffrement d'un message

2.6 Signature du fichier

3 Attaque décortiquée