Cryptographie & Sécurité

TP7

**Exercice 1**

**1 –**

On cherche  :

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

On cherche

On a donc comme clé publique le tuple et comme clé privée .

**2 –**

On cherche à envoyer le message avec la clé publique

Le message à envoyer est donc :

On cherche .

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

On prend et on trouve

Pour trouver , il est nécessaire de connaître

On a comme clé privée .

On retrouve bien .

**Exercice 2**

1 –

On a et .

2 –

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

On prend et on trouve .

3 –

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

On constate que donc .

On a bien .

**Exercice 3**

1 –

On choisit

Donc

2 –

On a

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

On obtient

3 –

On a donc bien .

**Exercice 4**

1 –

Les algorithmes étudiés ne sont pas infaillibles :

* Par exemple, RSA n’est pas infaillible pour des valeurs de et et de petites valeurs de , risquant inférieur à , et rendant la décryption simple. Aussi pour de petites valeurs de , on peut facilement (relativement parlant) trouver et et ainsi et donc à partir de .
* Pour l’algorithme Rabin, pour être certain que le choisi soit le bon parmi les 4 calculés, on doit vérifier à partir du message original, ce qui rend l’opération inefficace.  
  De plus, les et primes utilisés sont congrus à , ce qui réduit les nombres premiers candidats.  
  Avec un message crypté et un message potentiel, il est aisé de déterminer si oui ou non le cyphertext et le message correspondent.
* Dans le cas de ElGamal on constate que pour une clé provenant d’un possiblement inconnu, on peut facilement construire un message à partir d’une clé .

2 –

La résistance de ces algorithmes dépend premièrement de la taille des utilisés (qui influe directement sur le calcul des inverses modulaires et autres ) et ensuite de la modification apportée pré-encryption au message (padding et autres transformation linéaires).

On aurait donc dû utiliser un padding ainsi que des valeurs considérablement plus grandes pour et .

En admettant la possibilité qu’un algorithme de factorisation d’entiers efficace soit crée dans le futur, ces algorithmes pourraient devenir poreux (sans parler du hype train/nid de poule scientifique que représente la computation quantique dans la majorité des conversations centrées sur le domaine de la cryptographie).