# TD6 — Extras

*Comme au contrôle terminal, il est recommandé de se munir d'une calculatrice pour traiter certains de ces exercices.*

**Ex1. Attaque contre Diffie-Hellman**

Diffie-Hellman est un processus permettant à deux individus d'établir une donnée secrète partagée à partir de données publiques $g$ et $n$. Pour rappel, Diffie-Hellman se déroule en trois étapes entre Alice et Bob.

1. Alice choisit un entier au hasard $a$ et calcule $x = g^a \mod n$. En parallèle, Bob choisit également un entier au hasard $b$ et calcule $y = g^b \mod n$.
2. Alice et Bob s'échangent les valeurs $x$ et $y$. L'échange se fait *publiquement* (canal non sécurisé), et concerne uniquement les deux valeurs $x$ et $y$ ; en particulier, les entiers $a$ et $b$ ne sont pas communiqués.
3. Alice et Bob calculent, chacun de leur côté, le secret partagé $K = g^{a*b} \mod n$.
   (a) Alice calcule $K = y^a \mod n$
   (b) Bob calcule $K = x^b \mod n$

Suite à ces trois étapes, Alice et Bob sont les seuls à connaître leur secret partagé K. Posons maintenant $n = 2^k$ pour $k > 8$ et $g$ premier avec $n$. La donnée secrète partagée est donc représentable par une suite de $k$ bits.
Alice et Bob peuvent alors discuter de manière sécurisée de la façon suivante :

3. Alice envoie à bob $m_1 \oplus hex(K), \ldots, m_j \oplus hex(K)$ où les $m_i$ sont des blocs de $k$ bits représentés sous leur forme hexadécimale, $m = m_1, \ldots, m_j$ et $hex(K)$ représente K sous la forme hexadécimale.

Comme mentionné en cours, il existe une attaque dite *man-in-the-middle*. Pour une troisième personne (ici Yoh), le but est de se faire passer pour Bob auprès d'Alice et d'Alice auprès de Bob. Au final, les deux pensent communiquer entre eux et techniquement c'est le cas, sauf que Yoh a réussi à connaître l'information secrète en étant actif au moment de l'établissement de cette information secrète. On suppose ici que Yoh peut intercepter des messages et peut envoyer des messages à n'importe qui. De plus, personne ne peut vraiment vérifier l'origine du message. Voici les faits que nous connaissons :

- $g = 3$
- $n = 2^{12} = 4096$
- Alice a généré le nombre aléatoire 383 ;
- Bob a généré le nombre aléatoire 266 ;
- Yoh a généré le nombre aléatoire 370.

Les messages suivants ont transité sur le réseau : $message_1$ =1195, $message_2 = 3273$, $message_3 = 2729$ et $message_4 =$ `cd2, c2e`. On sait que $message_4$ a été envoyé par Bob. On connaît également les carrés successifs de 3 en base 4096 :

**Questions :**

1. Recontextualiser les messages (qui envoie le message à qui) et ordonnez les pour réaliser l'attaque de Yoh. Vous pouvez appliquer la méthode vue dans la vidéo récente à ce sujet avec Alice d'un côté, Bob de l'autre et l'homme du milieu. La question finalement ici est de savoir qui a envoyé quoi et à quel moment.

2. Déchiffrez alors le contenu de $message_4$.

**Ex2. El-Gamal - 4 pts**

Nous avons les données publiques : $n$ et $g$. Alice et Bob sont deux étudiants de master 1 (MIAGE ou Info, qui sait ?). Ils ont appliqué l'algorithme vu en cours de la façon suivante :

1. Alice choisit un entier au hasard $a$ et calcule $x = g^a \mod n$. En parallèle, Bob choisit également un entier au hasard $b$ et calcule $y = g^b \mod n$.

2. Alice envoie alors Bob : $g^a$

3. Bob calcule $K = x^b = g^{a*b} \mod n$. Il prend un message $m$ une chaîne de caractères (ou chaque caractère est codé sur un seul octet). Il construit le message chiffre $c$ de la façon suivante : $c = [(K*ord(y)) \ \% \ n \text{ for } y \text{ in } m]$. Pour illustrer cette notation issue de Python, prenons $m$ ="top", $K = 28$ et $n = 311$. Dans ce cas là, $c = [138, 309, 26]$ avec

   - $28*ord("t") \mod 311 = 28*(74hex) = 28*(7*16^1+4*16^0) = 28*116 \mod 311 = 138$
   - $28*ord("o") \mod 311 = 28*(6Fhex) = 28*(6*16^1+15*16^0) = 28*11 \mod 311 = 309$
   - $28*ord("p") \mod 311 = 28*(70hex) = 28*(7*16^1+0*16^0) = 28*112 \mod 311 = 26$

   En résumé, il envoie $(y, c)$ où $y$ a bien été calculé lors de l'étape 1.

4. Alice, comme d'habitude, va aussi calculer K. Puis elle va s'attaquer au déchiffrement en traitant un à un les entiers reçus. Cette opération lui permettra d'obtenir les octets originaux (et donc les caractères).

Dans le cas ci dessous, nous avons les données publiques : $n = 257$ et $g = 3$. Vous êtes également un étudiant et vous avez récupéré les indices suivants :

1. Alice a envoyé 135 ;

2. Bob a envoyé $(143, [81, 56])$.

Alice et Bob ne sont pas très doués en programmation. Ils ont fait les calculs à la main avec les algorithmes vus en cours. Dans les papiers d'Alice, vous avez retrouvé la note suivante : $9 * 136 * 249 * 64 = 135$. Étrangement, vous avez trouvé quelque chose d'équivalent dans les papiers de Bob : $9 * 81 * 136 * 64 = 143$.

**Questions :**

1. Question préliminaire : convertissez la valeur décimale **77** en hexadécimal. Quel caractère se cache derrière cette valeur ?

2. A partir de toutes les infos que vous avez récupérées, quel est le message secret envoyé par Bob ? Décrivez très exactement votre méthodologie.

## Annexe

- Carrés successifs en base 106481 :
  - 102769, 42895, 95826, 20279, 8219, 43007, 27079, 44075
  - 15763, 51996, 31426, 88682, 23426, 80883, 80011, 15920

- 91231, 7996, 47416, 37222, 52993, 34636, 37550, 87579

- Produits utiles en base 106481 : 8219 * 102769 = **51119**; 15763 * 80883 = **61716**; 15920 * 61716 = **18533**; 18471 * 37222 = **86226**; 27079 * 68107 = **18533**; 37550 * 86226 = **18533**; 43007 * 51119 = **68107**; 47416 * 91231 = **18471**

- Quelques conversions de nombres décimaux en hexadécimal : $38 \mapsto_{hex} 026$, $258 \mapsto_{hex} 102$, $415 \mapsto_{hex} 19f$, $615 \mapsto_{hex} 267$, $3857 \mapsto_{hex} f11$, $449 \mapsto_{hex} 1c1$, $195 \mapsto_{hex} 0c3$, $394 \mapsto_{hex} 18a$, $307 \mapsto_{hex} 133$, $289 \mapsto_{hex} 121$, $345 \mapsto_{hex} 159$

- Produits utiles en base 4096 : 3 * 9 = **27**; 9 * 1857 = **329**; 9 * 2465 = **1705**; 27 * 81 = **2187**; 1017 * 2689 = **2681**; 1025 * 1705 = **2729**; 1025 * 2219 = **1195**; 1025 * 2249 = **3273**; 1185 * 3353 = **185**; 1209 * 2081 = **985**; 1281 * 2681 = **1913**; 1489 * 3273 = **3353**; 1489 * 3393 = **1809**; 1809 * 2049 = **3857**; 185 * 3393 = **1017**; 1913 * 2561 = **377**; 2049 * 3481 = **1433**; 2177 * 3609 = **665**; 2187 * 2465 = **619**; 2241 * 2617 = **3321**; 2457 * 3073 = **1433**; 2475 * 3329 = **2219**; 257 * 1041 = **1297**; 257 * 665 = **2969**; 2603 * 3713 = **2475**; 2617 * 2657 = **2457**; 3073 * 3449 = **2425**; 329 * 3713 = **969**; 377 * 2049 = **2425**; 385 * 3321 = **633**; 513 * 1297 = **1809**; 513 * 2969 = **3481**; 619 * 1857 = **2603**; 633 * 769 = **3449**; 913 * 2177 = **1041**; 913 * 2729 = **1209**; 969 * 3329 = **2249**; 985 * 1089 = **3609**

- Carrés successifs en base 4096 :
  - 3, 9, 81, 2465, 1857, 3713, 3329, 2561, 1025, 2049, 1, 1, ...
  - 1195, 2617, 177, 2657, 2241, 385, 769, 1537, 3073, 2049, 1, ...
  - 2729, 913, 2081, 1089, 2177, 257, 513, 1025, 2049, 1, ...
  - 3273, 1489, 1185, 3393, 2689, 1281, 2561, 1025, 2049, 1, ...

- Carrés utiles en base 257 :
  - 3, 9, 81, 136, 249, 64, 241, 256, 1, ...
  - 143, 146, 242, 225, 253, 16, 256, 1, ...
  - 135, 235, 227, 129, 193, 241, 256, 1, ...

- Produits utiles en base 257 : 6 * 134 = **33**; 129 * 146 = **73**; 137 * 134 = **111**; 146 * 225 = **211**; 158 * 134 = **98**; 16 * 184 = **117**; 18 * 134 = **99**; 20 * 134 = **110**; 211 * 253 = **184**; 22 * 134 = **121**; 227 * 235 = **146**; 252 * 134 = **101**; 41 * 134 = **97**; 43 * 134 = **108**; 56 * 134 = **51**; 60 * 134 = **73**; 73 * 241 = **117**; 81 * 134 = **60**; 85 * 134 = **82**

| Hex | Char | Hex | Char | Hex | Char | Hex | Char | Hex | Char | Hex | Char |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 20 | *espace* | 30 | 0 | 40 | @ | 50 | P | 60 | ` | 70 | p |
| 21 | ! | 31 | 1 | 41 | A | 51 | Q | 61 | a | 71 | q |
| 22 | " | 32 | 2 | 42 | B | 52 | R | 62 | b | 72 | r |
| 23 | # | 33 | 3 | 43 | C | 53 | S | 63 | c | 73 | s |
| 24 | $ | 34 | 4 | 44 | D | 54 | T | 64 | d | 74 | t |
| 25 | % | 35 | 5 | 45 | E | 55 | U | 65 | e | 75 | u |
| 26 | & | 36 | 6 | 46 | F | 56 | V | 66 | f | 76 | v |
| 27 | ' | 37 | 7 | 47 | G | 57 | W | 67 | g | 77 | w |
| 28 | ( | 38 | 8 | 48 | H | 58 | X | 68 | h | 78 | x |
| 29 | ) | 39 | 9 | 49 | I | 59 | Y | 69 | i | 79 | y |
| 2A | * | 3A | : | 4A | J | 5A | Z | 6A | j | 7A | z |
| 2B | + | 3B | ; | 4B | K | 5B | [ | 6B | k | 7B | { |
| 2C | , | 3C | < | 4C | L | 5C | \ | 6C | l | 7C | \| |
| 2D | - | 3D | = | 4D | M | 5D | ] | 6D | m | 7D | } |
| 2E | . | 3E | > | 4E | N | 5E | ^ | 6E | n | 7E | ~ |
| 2F | / | 3F | ? | 4F | O | 5F | _ | 6F | o | | |

Figure 1: ASCII

| XOR | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **0** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| **1** | 1 | 0 | 3 | 2 | 5 | 4 | 7 | 6 | 9 | 8 | B | A | D | C | F | E |
| **2** | 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 | A | B | 8 | 9 | E | F | C | D |
| **3** | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | B | A | 9 | 8 | F | E | D | C |
| **4** | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | C | D | E | F | 8 | 9 | A | B |
| **5** | 5 | 4 | 7 | 6 | 1 | 0 | 3 | 2 | D | C | F | E | 9 | 8 | B | A |
| **6** | 6 | 7 | 4 | 5 | 2 | 3 | 0 | 1 | E | F | C | D | A | B | 8 | 9 |
| **7** | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | F | E | D | C | B | A | 9 | 8 |
| **8** | 8 | 9 | A | B | C | D | E | F | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **9** | 9 | 8 | B | A | D | C | F | E | 1 | 0 | 3 | 2 | 5 | 4 | 7 | 6 |
| **A** | A | B | 8 | 9 | E | F | C | D | 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 |
| **B** | B | A | 9 | 8 | F | E | D | C | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 |
| **C** | C | D | E | F | 8 | 9 | A | B | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| **D** | D | C | F | E | 9 | 8 | B | A | 5 | 4 | 7 | 6 | 1 | 0 | 3 | 2 |
| **E** | E | F | C | D | A | B | 8 | 9 | 6 | 7 | 4 | 5 | 2 | 3 | 0 | 1 |
| **F** | F | E | D | C | B | A | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

Figure 2: Table du $\oplus$