



6. Alice et Bob communiquent à l'aide d'une variation autour du protocole de Diffie-Hellman inspirée du schéma de chiffrement ElGamal. On suppose n et g publiquement connus avec n premier. Alice dispose d'un message m qu'elle souhaite transmettre de manière confidentielle à Bob. Le protocole est le suivant :
1. Alice choisit secrètement a et calcule $x = g^a \pmod{n}$. Elle envoie x à Bob.
 2. Bob choisit secrètement b et calcule $y = g^b \pmod{n}$. Il envoie y à Alice.
 3. Alice calcule $c = m \times y^a \pmod{n}$. Elle envoie c à Bob.
- a. Expliquer comment Bob peut calculer efficacement m à partir des informations dont il dispose, à savoir n, g, x, b et c . Détailler l'algorithme et justifier la facilité de calcul.
- b. Calculer le message m correspondant à $n = 5003, g = 5, x = 3949, b = 257, y = 180, c = 3073$. Indiquer les calculs sur la copie.
- c. Eve a la capacité d'intercepter les messages qui circulent entre Alice et Bob et d'émettre des messages en se faisant passer pour Alice auprès de Bob et Bob auprès d'Alice. Expliquer comment Eve peut intervenir dans les échanges pour être capable elle aussi de calculer m . Justifier.
- d. Améliorer le protocole d'Eve pour assurer qu'à la fin du protocole, Bob reçoit bien lui aussi le message d'Alice et ne se doute de rien.

Outils divers

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Puissances de 2 : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, 2097152, 4194304, 8388608, 16777216, 33554432, 67108864, 134217728, 268435456, 536870912, ...

Premiers premiers : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227.

Suite de carrés successifs modulo 5003 (*i.e.* $u_{n+1} = (u_n^2 \bmod 5003)$) :

5, 25, 625, 391, 2791, 10, 100, 4997, 36, 1296, 3611, 1503, 2656, 106, 1230, 1994, 3654, 3712, 682, 4848, ...
 180, 2382, 522, 2322, 3453, 1060, 2928, 3045, 1466, 2869, 1226, 2176, 2138, 3305, 1476, 2271, 4351, 4852, 2789, 3859, ...
 257, 1010, 4491, 1988, 4777, 1046, 3462, 3259, 4715, 2896, 1788, 27, 729, 1123, 373, 4048, 1479, 1130, 1135, 2454, ...
 3073, 2668, 3958, 1371, 3516, 4846, 4637, 3878, 4869, 2947, 4604, 4108, 545, 1848, 3058, 757, 2707, 3457, 3685, 1083...
 3949, 250, 2464, 2657, 416, 2954, 884, 988, 559, 2295, 3869, 185, 4207, 3238, 3359, 1116, 4712, 4633, 1819, 1778, ...

Quelques produits modulo 5003 : $180 \times 257 = 1233$, $180 \times 2029 = 1$, $257 \times 3073 = 4290$, $257 \times 4711 = 1$, $559 \times 3949 = 1168$, $1168 \times 3688 = 1$, $2029 \times 3073 = 1379$, $3073 \times 4711 = 3224$, $3073 \times 3688 = 1429$.

Quelques produits modulo 8453 : $4 \times 6144 = 7670$, $3564 \times 7670 = 7331$, $3636 \times 3636 = 4$, $3636 \times 5916 = 6144$, $3766 \times 7113 = 1$, $5916 \times 5916 = 3636$, $7113 \times 7113 = 3564$.



6. Alice et Bob communiquent à l'aide d'une variation autour du protocole de Diffie-Hellman inspirée du schéma de chiffrement ElGamal. On suppose n et g publiquement connus avec n premier. Alice dispose d'un message m qu'elle souhaite transmettre de manière confidentielle à Bob. Le protocole est le suivant :
1. Alice choisit secrètement a et calcule $x = g^a \pmod{n}$. Elle envoie x à Bob.
 2. Bob choisit secrètement b et calcule $y = g^b \pmod{n}$. Il envoie y à Alice.
 3. Alice calcule $c = m \times y^a \pmod{n}$. Elle envoie c à Bob.
- a. Expliquer comment Bob peut calculer efficacement m à partir des informations dont il dispose, à savoir n, g, x, b et c . Détailler l'algorithme et justifier la facilité de calcul.
- b. Calculer le message m correspondant à $n = 5003, g = 5, x = 3949, b = 257, y = 180, c = 3073$. Indiquer les calculs sur la copie.
- c. Eve a la capacité d'intercepter les messages qui circulent entre Alice et Bob et d'émettre des messages en se faisant passer pour Alice auprès de Bob et Bob auprès d'Alice. Expliquer comment Eve peut intervenir dans les échanges pour être capable elle aussi de calculer m . Justifier.
- d. Améliorer le protocole d'Eve pour assurer qu'à la fin du protocole, Bob reçoit bien lui aussi le message d'Alice et ne se doute de rien.

Outils divers

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Puissances de 2 : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, 2097152, 4194304, 8388608, 16777216, 33554432, 67108864, 134217728, 268435456, 536870912, ...

Premiers premiers : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227.

Suite de carrés successifs modulo 5003 (*i.e.* $u_{n+1} = (u_n^2 \bmod 5003)$) :

5, 25, 625, 391, 2791, 10, 100, 4997, 36, 1296, 3611, 1503, 2656, 106, 1230, 1994, 3654, 3712, 682, 4848, ...
 180, 2382, 522, 2322, 3453, 1060, 2928, 3045, 1466, 2869, 1226, 2176, 2138, 3305, 1476, 2271, 4351, 4852, 2789, 3859, ...
 257, 1010, 4491, 1988, 4777, 1046, 3462, 3259, 4715, 2896, 1788, 27, 729, 1123, 373, 4048, 1479, 1130, 1135, 2454, ...
 3073, 2668, 3958, 1371, 3516, 4846, 4637, 3878, 4869, 2947, 4604, 4108, 545, 1848, 3058, 757, 2707, 3457, 3685, 1083...
 3949, 250, 2464, 2657, 416, 2954, 884, 988, 559, 2295, 3869, 185, 4207, 3238, 3359, 1116, 4712, 4633, 1819, 1778, ...

Quelques produits modulo 5003 : $180 \times 257 = 1233$, $180 \times 2029 = 1$, $257 \times 3073 = 4290$, $257 \times 4711 = 1$, $559 \times 3949 = 1168$, $1168 \times 3688 = 1$, $2029 \times 3073 = 1379$, $3073 \times 4711 = 3224$, $3073 \times 3688 = 1429$.

Quelques produits modulo 8453 : $4 \times 6144 = 7670$, $3564 \times 7670 = 7331$, $3636 \times 3636 = 4$, $3636 \times 5916 = 6144$, $3766 \times 7113 = 1$, $5916 \times 5916 = 3636$, $7113 \times 7113 = 3564$.