El criptosistema ElGamal

Artur Travesa

(versió 2021-04)

Introducció general

L'origen d'aquestes notes es remunta a diferents cursos d'Aritmètica o de Criptografia, a càrrec de l'autor, per a estudiants de Matemàtiques o d'Informàtica de la Universitat de Barcelona.

La idea bàsica és descriure algunes aplicacions importants de l'Aritmètica bàsica (diguem, de nivell de primer curs) a les transmissions xifrades d'informació.

En cap cas es tracta d'un curs de Criptografia, que caldria encabir en espais més amplis de coneixements, que haurien d'incloure, probablement, parts de teoria de la comunicació, de complexitat algorítmica o computacional, d'aprenentatge automàtic, o d'estudi de teories de compartició de secrets, entre d'altres.

El format triat per a la presentació és el d'un *notebook* de *Mathematica*, per la facilitat que té aquest programari per a poder desenvolupar els càlculs no trivials de manera prou senzilla i entenedora, d'una banda, i per a permetre fer una presentació escrita prou raonable des del punt de vista de material escrit, de l'altra. En particular, la possibilitat d'incloure els càlculs dins del text de manera natural en fan una bona eina comunicativa i, alhora, facilita molt el càlcul amb exemples no trivials.

A fi de veure tot el contingut del *notebook* convé executar-lo. Això es pot fer de cop o bé, més recomanable, cel·la a cel·la a mesura que s'avança en la lectura i comprensió dels diferents continguts.

Observació: Per al cas en què no es disposi del programari, hi ha la versió executada del *notebook* en format pdf.

Amb la finalitat doble d'una banda, de no fer textos molt llargs o amb molts continguts, i de l'altra de poder ampliar de manera senzilla els continguts que s'hi tractin, el material s'ha dividit en diferents *notebooks*, que desrivim a continuació, en l'apartat de referències.

Referències

[Cripto- 1]: **Criptografia bàsica (1)**.
Travesa, A.: CriptografiaBasica-1; accessible en forma notebook o en format pdf des de https://travesa.cat/notes/
Contingut: Una iniciació a la codificació de missatges. El criptosistema de Cèsar. El criptosistema de Vigenère.

[Cripto- 2]: **Criptografia bàsica (2)**.
Travesa, A.:CriptografiaBasica-2; accessible en forma notebook o en format pdf des de https://travesa.cat/notes/
Contingut: Els criptosistemes lineals. Els criptosistemes afins. Sufixació de missatges. Farciment de missatges.

[Eratostenes]: **Un garbell d'Eratòstenes.**
Travesa, A.: Eratostenes; accessible en forma notebook o en format pdf des de https://travesa.cat/notes/
Contingut: Un garbell d'Eratòstenes.

[Cripto- 3]: **Primeritat. Construcció de primers**.
Travesa, A.: ConstruccioDePrimers; accessible en forma notebook o en format pdf des de https://travesa.cat/notes/
Contingut: Test de primeritat de Solovay-Strassen. Test de primeritat de Miller-Rabin. Un certificat congruencial de primeritat. Construcció certificada de nombres primers de mida prefixada. Aplicació al càlcul de claus RSA. Aplicació (exercici) al càlcul de claus ElGamal.

[Cripto- 4]: **Factorització**.
Travesa, A.: Factoritzacio; accessible en forma notebook o en format pdf des de https://travesa.cat/notes/
Contingut: Un garbell d'Eratòstenes. Tests de primeritat de Solovay-Strassen i de Miller-Rabin. Un certificat congruencial de primeritat. Un algoritme bàsic de divisó per nombres primers petits. Un algoritme bàsic de divisó per nombres petits. El mètode de factorització de Fermat. El mètode de factorització p-1 de Pollard. El mètode de factorització rho de Pollard.

[RSA]: **Criptosistemes de tipus RSA**.
Travesa, A.: RSA; accessible en forma notebook o en format pdf des de https://travesa.cat/notes/
Contingut: Una descripció bàsica dels criptosistemes de tipus RSA: les claus; xifratge; desxifratge; observacions sobre la seguretat.

[ElGamal]: **El criptosistema ElGamal**.
Travesa, A.: ElGamal; accessible en forma notebook o en format pdf des de https://travesa.cat/notes/
Contingut: Logaritmes discrets. Una descripció bàsica del criptosistema ElGamal: el grup cíclic; les claus; xifratge i desxifratge.

[D- H]: Diffie, W.; Hellman, M.E.: New directions in cryptography, *IEEE Transactions on Information Theory*, **22** (1976), p. 644- 654.

[ElGamal- 1]: ElGamal, T.: A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, **31** (1985), p. 469-472.

[DSS- Standard]: FIPS PUB 186-4: Digital Signature Standard (DSS). *Federal Information Processing Standards Publication.* National Institute of Standards and Technology, 2013.

[Tr-1]: Travesa, A.: *Aritmetica*. Edicions de la Universitat de Barelona, col·lecció UB, n. 25. Barcelona, 1998. ISBN:84-8338-031-5.

Introducció

El criptosistema **ElGamal** és basat en el mateix principi que el protocol **Diffie- Hellman** per a intercanvi de claus en canals públics; el va inventar Tahe ElGamal, que el va descriure en un article en 1984 (cf. **[D- H]**, **[ElGamal- 1]** a les referències). És la base d'un dels estàndards actuals (DSA) de signatura digital (cf. **[DSS- Standard,** cap. 4**]**).

La seguretat del criptosistema ElGamal es basa en la dificultat (conjectural) de calcular logaritmes discrets arbitraris. En efecte, donats un nombre primer p, un element g invertible mòdul p, i un nombre natural x, el càlcul de la potència, $h=g^x \pmod p$ es pot fer en temps polinòmic en la longitud en bits de p i x; en canvi, no es coneix cap algoritme tal que, donats p, g i h, trobi el nombre x en temps polinòmic en la longitud en bits de p (com en el cas de la factorització, el millor algoritme que es coneix actualment és subexponencial).

En farem una descripció i, simultàniament, un exemple.

1. Logaritmes discrets

En general, suposem que disposem d'un grup qualsevol, G, i d'un element $g \in G$ d'ordre finit, q. Escriurem multiplicativament l'operació del grup i ens fixarem en el subgrup cíclic de G generat per g. Aquest subgrup, C_g, és format per les potències $h=g^x$, per a $1 \leq x \leq q$, ja que q és l'ordre de g; notem, també, que $g^0=g^q=1$ és l'element neutre del grup G i, per tant, també del grup C_g.

Definició

Amb les notacions anteriors, i per analogia amb els logaritmes reals o complexos, x s'anomena el logaritme discret de h en base g. Notem que x és un nombre enter, que està definit mòdul l'ordre q de g en G; per tant, podem pensar x com un element de $\mathbb{Z}/q\mathbb{Z}$.

Obervació 1

Així, l'assignació $x \to g^x$ defineix un isomorfisme (de grups) entre el grup additiu $\mathbb{Z}/q\mathbb{Z}$ i el grup multiplicactiu C_g: l'exponencial de base g.

Exemple

Considerem un nombre natural primer p, i sigui G el grup dels elements invertibles mòdul p. En G, podem considerar qualsevol element g com a base dels logaritmes discrets. Si anomenem q l'ordre de g, tenim que el grup C_g és format per les potències $h=g^x$, per a $1 \leq x \leq q$. També tenim que, en virtut del petit teorema de Fermat, q és un divisor de p- 1.

Observació 2

En general, donats p, g, i $g^x \pmod p$, el càlcul de x no se sap fer en temps polinòmic respecte de la mida en bits de p (ni tan sols, conegut q).

Observació 3

Notem que si en lloc de considerar el grup multiplicatiu dels elements invertibles mòdul n, considerem tot el grup additiu de les classes residuals mòdul n, i g és una classe qualsevol, la potència g^x de més amunt es correspon ara amb el producte $g \cdot x$, de manera que el càlcul del logaritme discret es redueix a la resolució de la congruència lineal $g \cdot x = h \pmod{n}$; i aquesta es pot resoldre (mitjançant l'algoritme d'Euclides, per exemple) en temps polinòmic en la longitud en bits de n. Per tant, hi ha grups cíclics per als quals el problema del logaritme discret és polinomic.

2. La base del criptosistema ELGamal

El grup cíclic

De manera similar a com en els criptosistemes de tipus RSA la base del mètode és el càlcul de potències mòdul un nombre enter N, així també en el criptosistema ElGamal la base és aquest mateix tipus de càlcul.

Cada usuari U del criptosistema tria un nombre primer senar p i un nombre enter g no divisible per p i tal que l'ordre multiplicatiu de g en $(\mathbb{Z}/p\mathbb{Z})^*$ sigui un nombre primer senar q. (Moltes vegades, tots els usuaris U del criptosistema utilitzen el mateixos valors de p i g i, per tant, tots coneixen també el valor de q.)

En particular, es té que $p - 1 = 2 \cdot k \cdot q$, on k és un nombre enter. D'aquesta manera, el subgrup G de $(\mathbb{Z}/p\mathbb{Z})^*$ generat per g és cíclic, d'ordre primer, q, i és format pels elements g^x, $1 \leq x \leq q$, de $(\mathbb{Z}/p\mathbb{Z})^*$.

Observació 4

A fi que aquesta tria sigui útil per al criptosistema ElGamal cal que el problema del logaritme discret en el grup G sigui computacionalment intractable, encara que aquesta condició no és l'única que cal per a G. (A la pràctica, si no es fa servir tot $(\mathbb{Z}/p\mathbb{Z})^*$ en lloc de G, i una arrel primitiva mòdul p en lloc de g, és per a satisfer la necessitat d'aquesta condició.)

Observació 5

En l'actualitat (abril de 2021), sembla prou segur utilitzar nombres primers p tals que l'ordre de G, posem q, sigui un nombre d'un miler de bits, aproximadament. En el nostre exemple, prendrem com a p un nombre primer de 1024 bits i tal que p-1 sigui divisible per un primer q de 1000 bits. D'aquesta manera, el nombre enter $k := \frac{p-1}{2 \cdot q}$ serà un nombre de, com a màxim, 24 bits, o sigui, relativament petit.

Observació 6

El càlcul de nombres p, q i k en aquestes condicions no és especialment complicat, i es pot fer a partir d'algoritmes probabilístics. Per exemple, es pot consultar la referència **[Cripto- 3]**.

Observació 7

D'altra banda, la tria d'un element de $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre q no presenta dificultats. En efecte, si g_0 és una arrel primitiva mòdul p, l'element $g_0^{2 \cdot k}$ és d'ordre q, i tots els elements de $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre q són de la forma $g_0^{2 \cdot k}$, per a alguna arrel primitiva mòdul p, g_0. Per tant, és suficient calcular una arrel primitiva mòdul p i elevar aquesta a la potència $2 \cdot k$, mòdul p.

Exercici 1

(a) Es demana calcular un nombre primer p de 1024 bits de manera que p-1 sigui el producte d'un nombre primer q de 1000 bits per un nombre enter parell $2 \cdot k$.
(b) Es demana calcular un element g de $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre q, per als valors p, q de l'apartat (a).

3. Les claus

Les claus

Quan l'usuari U disposa de p, q, k i g, tria a l'atzar un nombre enter x, $1 \leq x \leq q$-1, i calcula $h := g^x \pmod p$. D'aquesta manera, h és un element de G.

Definició.

La **clau pública** de U és (p, q, g, h); la **clau privada** de U és (p, q, g, x). Notem que l'única diferència és en h i x, mentre que els paràmetres p, q i g són comuns; en particular, tots els usuaris del criptosistema poden usar els mateixos p, q, i g.

Observació 8

Els nombres h i x de les claus juguen un paper molt diferent. Així com h és un element de G, i actua com a tal en el procés de xifratge, x és un nombre natural, i actua com a tal en el procés de desxifratge. En conseqüència, x i h no són intercanviables, en contraposició a les claus pública i privada del criptosistema RSA, que sí que són intercanviables.

Observació 9

Cal notar que calcular x a partir de p, q, g i h vol dir calcular el logaritme discret mòdul p, de base g, per a l'element h; per tant, si no podem resoldre aquest problema de logaritme discret, no sabem calcular la clau privada de U a partir de la seva clau pública.

Exercici 2

Es demana crear, a partir dels nombres p, q i g de l'exercici 1, una parella de claus pública (p, q, g, h) i privada (p, q, g, x) per al criptosistema ElGamal. Les anomenarem ***ClauElGamalPublica*** i ***ClauElGamalPrivada***.

4. Xifratge i desxifratge

Xifratge

Les unitats de missatge que es poden xifrar amb el criptosistema ElGamal són els elements de $\mathbb{Z}/p\mathbb{Z}$. En particular, el conjunt d'unitats de missatge vàlides és diferent per a cada usuari si cadascun treballa en un anell diferent, però el mateix si tots els usuaris treballen amb el mateix valor de p; és per això que és còmode usar el mateix valor de p per a tots els usuaris del criptosistema.

Notem que el conjunt de missatges que poden ser xifrats és més gran que el grup que fem servir per a xifrar; de fet, el grup G és un subgrup de $(\mathbb{Z}/p\mathbb{Z})^*$ que, alhora, és un subconjunt de $\mathbb{Z}/p\mathbb{Z}$.

Suposem que la unitat de missatge que es vol xifrar és un element m de $\mathbb{Z}/p\mathbb{Z}$, on p és el nombre primer de la clau de U. L'usuari V que vol enviar el missatge m a U, tria a l'atzar un nombre y de l'interval $1 \leq y \leq q\text{-}1$ i calcula els dos nombres $c_1 = g^y \pmod p$ i $c_2 = m \cdot h^y \pmod p$, amb $0 \leq c_1 \leq p - 1$, $0 \leq c_2 \leq p - 1$. El missatge xifrat associat a m és la parella de nombres naturals (c_1, c_2).

Observació 10

Cal notar que tant c_1 com c_2 són nombres de, com a màxim, 1024 bits, perquè p és de 1024 bits.

Desxifratge

Per a desxifrar el missatge, l'usuari U calcula el producte $c_2 \cdot {c_1}^{-x} \pmod p$; pot calcular-ho perquè coneix el valor secret x, i això produeix el missatge m.

Demostració.

En efecte, es té que $c_2 \cdot {c_1}^{-x} \pmod p = m \cdot h^y \cdot \left(g^y\right)^{-x} \pmod p = m \cdot \left(g^x\right)^y \cdot \left(g^y\right)^{-x} \pmod p = m \pmod p$, perquè $\left(g^x\right)^y \cdot \left(g^y\right)^{-x} = 1 \pmod p$. □

Observació 11

Cal notar que les potències de g són elements de $(\mathbb{Z}/p\mathbb{Z})^*$, de manera que la multiplicació per ells (i pels seus inversos) és possible a tot $\mathbb{Z}/p\mathbb{Z}$, i no cal restringir-se a G.

Exemple

La funció següent pren com a entrades una llista d'unitats de missatge i una clau pública ElGamal i produeix una llista d'unitats de missatge xifrades amb aquesta clau pública.

```
ElGamalX0[mc_, claupublica_] := Module[{l, p, q, g, h},
  l = Length[mc];
  {p, q, g, h} = claupublica; Table[Module[{y}, y = RandomInteger[{1, q - 1}];
    {PowerMod[g, y, p], Mod[mc[[i]] PowerMod[h, y, p], p]}], {i, 1, l}]]
```

Observem que, un cop hem resolt l'exercici 2, ja disposem d'una parella de claus pública i privada per al criptosistema ElGamal. Suposem que la clau pública és en una llista anomenada ***ClauElGamalPublica*** i que la clau privada és en una llista anomenada ***ClauElGamalPrivada***. (Per si encara no s'ha resolt l'exercici 2, aquí disposem d'una parella de claus pública i privada de 1024 bits per al criptosistema ElGamal.)

```
ClauElGamalPublica0 =
  {163 373 482 070 616 520 482 398 310 743 692 947 258 024 187 555 006 096 588 812 482 689 760 854 417 ∴
    440 048 731 392 326 852 427 737 973 179 256 721 612 890 171 131 756 272 531 583 884 786 837 102 571 ∴
    158 146 032 501 965 840 739 494 944 090 227 433 277 986 225 038 717 015 744 064 685 587 300 523 281 ∴
    291 737 140 262 198 891 946 817 108 834 786 035 512 782 165 528 962 112 703 335 943 007 934 782 543 ∴
    013 663 987,
   8 983 415 049 707 492 366 013 947 929 288 770 154 408 080 378 818 865 098 827 143 174 875 922 113 435 ∴
    731 308 268 597 717 117 906 608 851 477 886 358 229 103 001 275 163 145 368 973 373 588 778 441 668 ∴
    770 617 094 835 602 705 155 884 475 548 301 791 772 112 000 497 798 032 151 367 157 181 752 287 886 ∴
    979 815 722 241 327 312 486 802 234 956 195 472 172 801 080 349 186 742 689 614 806 715 515 410 213,
  124 405 340 357 782 733 382 026 994 779 058 227 932 934 248 315 057 335 738 978 399 309 754 188 004 ∴
    187 222 926 637 460 946 631 915 652 593 529 565 790 661 312 284 519 379 103 898 970 862 683 237 930 ∴
    977 058 092 972 540 974 467 037 935 436 050 218 324 136 871 779 298 774 648 619 650 237 403 112 827 ∴
    624 131 348 105 999 303 958 508 167 481 127 630 204 548 567 268 816 006 517 698 562 476 647 693 745 ∴
    716 432 813,
  114 634 913 690 868 408 045 159 549 415 324 390 018 533 038 864 900 907 239 378 466 033 997 484 018 ∴
    459 815 096 166 888 158 503 233 172 824 344 476 414 885 424 837 171 965 516 241 228 660 874 334 194 ∴
    045 389 841 214 775 128 782 523 254 874 262 682 250 655 340 421 838 736 085 971 094 886 127 856 882 ∴
    421 570 368 896 444 892 744 172 958 999 112 584 463 457 220 622 094 255 555 062 909 086 506 118 545 ∴
    339 158 309};
```

```
ClauElGamalPrivada0 =
  {163 373 482 070 616 520 482 398 310 743 692 947 258 024 187 555 006 096 588 812 482 689 760 854 417 ∖
    440 048 731 392 326 852 427 737 973 179 256 721 612 890 171 131 756 272 531 583 884 786 837 102 571 ∖
    158 146 032 501 965 840 739 494 944 090 227 433 277 986 225 038 717 015 744 064 685 587 300 523 281 ∖
    291 737 140 262 198 891 946 817 108 834 786 035 512 782 165 528 962 112 703 335 943 007 934 782 543 ∖
    013 663 987,
   8 983 415 049 707 492 366 013 947 929 288 770 154 408 080 378 818 865 098 827 143 174 875 922 113 435 ∖
    731 308 268 597 717 117 906 608 851 477 886 358 229 103 001 275 163 145 368 973 373 588 778 441 668 ∖
    770 617 094 835 602 705 155 884 475 548 301 791 772 112 000 497 798 032 151 367 157 181 752 287 886 ∖
    979 815 722 241 327 312 486 802 234 956 195 472 172 801 080 349 186 742 689 614 806 715 515 410 213,
   124 405 340 357 782 733 382 026 994 779 058 227 932 934 248 315 057 335 738 978 399 309 754 188 004 ∖
    187 222 926 637 460 946 631 915 652 593 529 565 790 661 312 284 519 379 103 898 970 862 683 237 930 ∖
    977 058 092 972 540 974 467 037 935 436 050 218 324 136 871 779 298 774 648 619 650 237 403 112 827 ∖
    624 131 348 105 999 303 958 508 167 481 127 630 204 548 567 268 816 006 517 698 562 476 647 693 745 ∖
    716 432 813,
   7 398 067 442 430 323 695 275 948 907 811 118 942 407 247 488 858 854 439 508 534 974 115 728 282 472 ∖
    772 782 681 541 873 500 452 008 993 913 618 222 146 818 467 748 237 743 113 897 542 085 721 933 409 ∖
    850 390 391 973 051 876 790 900 148 552 794 830 357 663 742 146 502 508 146 847 362 910 707 198 047 ∖
    328 894 199 497 948 604 070 960 870 873 737 517 350 449 973 836 145 565 244 003 560 855 801 364 061};
```

```
pe0 = ClauElGamalPublica0[[1]]
```

```
163 373 482 070 616 520 482 398 310 743 692 947 258 024 187 555 006 096 588 812 482 689 760 854 417 440 048 731 392 326 852 427 737 973 179 256 721 ∖
 612 890 171 131 756 272 531 583 884 786 837 102 571 158 146 032 501 965 840 739 494 944 090 227 433 277 986 225 038 717 015 744 064 685 587 300 ∖
 523 281 291 737 140 262 198 891 946 817 108 834 786 035 512 782 165 528 962 112 703 335 943 007 934 782 543 013 663 987
```

Ara, ens inventem un missatge.

```
m1 = Table[RandomInteger[{0, pe0 - 1}], {i, 1, 5}]
```

```
{62 153 115 061 110 945 709 552 255 516 644 523 681 464 082 348 112 573 663 352 944 128 544 756 508 868 487 388 369 916 145 571 057 801 290 480 791 ⁞
  318 635 344 674 069 680 147 789 496 903 120 398 864 255 527 231 530 930 959 381 314 696 919 221 737 318 034 505 179 044 238 220 552 049 129 035 ⁞
  389 205 128 649 011 234 049 345 101 747 262 998 773 286 639 423 269 348 886 381 633 376 754 091 436 553 841 660 234 865,
 39 889 220 496 077 227 147 273 141 036 653 186 025 510 538 540 794 371 431 355 141 700 175 159 517 961 135 654 457 722 806 424 813 887 058 962 ⁞
  135 783 606 794 023 527 714 919 218 498 203 673 271 557 355 313 750 622 061 157 577 910 208 832 441 349 389 616 862 561 967 242 177 264 410 366 ⁞
  239 051 510 320 517 168 740 669 181 826 271 917 519 330 064 397 334 253 279 958 891 515 760 991 982 220 699 699 362 514 543,
 98 416 381 192 257 134 121 142 109 574 411 578 161 201 416 302 040 429 474 716 473 622 865 620 556 924 560 470 488 413 446 152 729 066 969 446 ⁞
  669 001 319 969 058 278 335 935 545 967 932 612 745 337 153 300 664 140 751 225 265 182 834 444 761 513 699 124 183 110 379 390 699 995 494 745 ⁞
  612 500 849 389 129 643 726 072 265 220 344 580 105 128 705 237 768 340 408 615 004 166 701 521 959 638 200 237 677 622 041,
 102 845 913 823 042 325 791 910 452 247 550 664 641 407 894 966 928 790 202 424 691 911 492 603 723 783 956 874 693 603 917 772 223 006 728 362 ⁞
  910 985 290 743 642 635 104 457 052 595 098 162 069 447 202 866 777 454 540 421 361 040 039 734 377 931 625 244 913 598 714 833 645 254 395 175 ⁞
  148 291 408 692 778 479 703 304 314 254 319 244 525 494 478 277 984 672 139 705 975 919 104 422 577 859 667 637 414 448 755,
 115 727 065 617 801 469 478 314 232 245 392 497 749 284 219 565 250 485 470 168 983 808 914 689 829 169 849 785 211 336 715 953 014 002 523 538 ⁞
  613 272 460 097 840 272 045 215 006 966 176 638 317 234 043 694 893 360 961 442 423 085 276 249 527 040 519 912 505 656 686 353 582 019 708 826 ⁞
  386 631 739 083 080 864 535 700 390 944 060 831 101 042 908 751 017 702 306 082 839 797 930 786 328 426 533 546 795 505 742}
```

I el xifrem amb la clau pública.

```
x1 = ElGamalX0[m1, ClauElGamalPublica0]
```

```
{{13 002 960 533 082 769 742 849 077 821 113 541 638 033 453 733 638 460 952 286 140 431 160 052 918 006 499 995 774 689 568 012 494 081 858 581 ↓
    431 299 365 325 641 634 790 695 232 423 137 367 626 510 227 543 596 296 713 787 951 731 128 400 220 036 670 013 984 049 714 098 913 865 242 295 ↓
    497 653 638 370 921 502 043 964 532 515 794 866 625 845 540 135 398 799 452 296 029 437 152 827 961 787 722 310 803 505 654,
   3 692 984 940 912 150 381 851 673 733 073 256 931 874 631 813 778 760 411 706 633 461 497 814 536 220 917 131 428 673 904 559 075 607 925 556 ↓
    594 953 979 556 075 027 359 449 666 083 874 941 249 692 966 008 106 944 314 599 472 132 883 202 707 700 659 768 937 161 247 550 410 692 873 324 ↓
    917 698 832 143 668 909 118 083 643 515 454 602 145 011 638 029 504 627 758 258 246 793 575 948 218 033 796 968 543 530 991},
  {120 090 539 158 241 042 959 357 552 994 990 341 871 328 275 359 699 408 924 534 351 315 406 960 283 186 560 728 728 525 778 032 329 577 677 090 ↓
    869 824 942 972 595 212 088 418 536 116 529 165 364 873 525 094 204 419 334 658 566 159 353 820 230 581 020 148 604 947 349 689 354 902 442 720 ↓
    716 765 718 745 395 970 955 907 662 612 311 057 119 400 386 138 345 208 477 099 255 592 472 552 268 974 453 299 385 295 759,
   76 770 582 043 453 997 410 872 840 212 216 449 636 761 509 657 135 833 029 565 852 731 636 043 877 470 474 148 533 691 165 654 217 939 923 801 ↓
    252 096 606 491 011 254 644 232 556 742 760 120 722 302 072 500 571 250 540 018 164 877 009 777 434 890 418 769 243 296 885 045 224 236 872 447 ↓
    236 130 926 295 565 068 410 993 333 359 262 152 154 084 655 276 260 546 351 105 093 699 718 594 919 019 832 584 078 426 882},
  {71 848 673 721 224 484 148 037 425 983 032 578 859 062 470 130 671 864 311 627 507 491 754 828 105 118 915 543 199 515 326 841 058 889 386 718 ↓
    433 453 320 161 854 871 696 062 790 872 152 820 922 771 552 666 618 248 225 315 141 906 472 595 941 593 360 677 016 462 439 016 060 058 029 287 ↓
    101 431 926 706 125 833 433 581 344 266 896 953 226 848 193 260 856 474 150 409 262 677 224 140 131 514 308 515 430 379 494,
   46 860 676 181 210 422 692 886 620 577 376 903 732 935 778 449 870 300 991 277 703 964 876 322 005 655 634 500 467 076 171 454 440 531 982 638 ↓
    368 150 073 988 679 593 072 359 292 640 012 427 714 754 332 333 102 662 174 512 249 343 709 376 677 426 341 475 382 726 149 177 542 372 862 941 ↓
    497 438 602 108 816 959 783 361 760 987 755 030 142 025 043 525 603 586 631 497 824 186 472 987 244 987 754 275 582 312 535},
  {2 487 016 536 376 829 865 592 221 552 836 038 688 061 749 604 579 285 569 334 575 065 803 587 990 457 298 487 149 041 187 041 937 105 488 515 ↓
    884 778 861 517 785 030 712 588 757 391 429 217 091 736 955 994 044 616 891 945 487 852 528 087 359 274 065 405 938 451 926 463 382 319 606 864 ↓
    361 537 366 390 629 048 299 047 847 889 669 452 997 413 424 844 408 510 376 650 541 115 885 598 818 224 944 617 924 378 070,
   116 872 988 367 931 954 169 265 298 208 630 490 822 605 555 467 883 427 353 379 320 346 720 206 790 054 737 330 787 392 368 926 767 309 065 282 ↓
    910 835 066 552 678 959 447 907 157 058 531 149 762 138 751 195 812 429 258 252 749 452 068 734 317 924 371 250 078 865 058 383 507 227 927 033 ↓
    573 967 424 657 117 476 120 197 096 534 884 864 696 609 725 934 831 841 168 748 097 417 377 319 968 311 680 222 020 719 627},
  {69 585 048 321 694 183 553 990 156 157 480 196 811 809 055 273 409 748 689 982 124 879 090 398 824 332 733 958 298 971 051 983 025 643 827 231 ↓
    451 314 027 745 712 590 474 405 963 704 151 615 706 303 895 422 265 947 413 328 755 059 866 147 469 594 727 815 938 051 282 321 457 937 909 525 ↓
    608 643 708 942 120 974 041 946 087 586 680 571 670 023 647 965 265 323 444 506 392 312 418 735 009 733 252 854 033 958 794,
   62 468 247 490 290 223 004 622 091 419 484 804 481 679 041 553 729 196 608 374 244 588 832 518 104 838 451 960 050 773 818 619 878 323 836 577 ↓
    344 552 822 067 575 925 723 868 620 641 134 033 757 404 925 582 470 873 964 393 746 962 524 068 828 157 769 384 939 591 610 533 400 179 511 730 ↓
    990 401 981 129 762 114 688 316 550 972 292 209 510 189 252 350 859 076 148 381 289 344 988 345 765 415 837 894 317 451 112}}
```

Exercici 3

Es demana definir una funció, ***ElGamalDx0***, per a desxifrar missatges xifrats amb la funció ***ElGamalX0***. Notem que cal produir, a la sortida, el missatge codificat en forma d'una llista d'elements de $\mathbb{Z}/p\mathbb{Z}$, on p és el nombre primer de la clau privada. Per a comprovar que funciona bé, es pot provar de desxifrar el missatge $x1$.

```
ElGamalDX0[mx_, clauprivada_] := Module[{l, p, q, g, x},
  l = Length[mx];
  {p, q, g, x} = clauprivada; Table[Mod[mx[[i, 2]] PowerMod[mx[[i, 1]], -x, p], p], {i, 1, l}]]
```

dx1 = ElGamalDX0[x1, ClauElGamalPrivada0]

```
{62 153 115 061 110 945 709 552 255 516 644 523 681 464 082 348 112 573 663 352 944 128 544 756 508 868 487 388 369 916 145 571 057 801 290 480 791 ∴
  318 635 344 674 069 680 147 789 496 903 120 398 864 255 527 231 530 930 959 381 314 696 919 221 737 318 034 505 179 044 238 220 552 049 129 035 ∴
  389 205 128 649 011 234 049 345 101 747 262 998 773 286 639 423 269 348 886 381 633 376 754 091 436 553 841 660 234 865,
 39 889 220 496 077 227 147 273 141 036 653 186 025 510 538 540 794 371 431 355 141 700 175 159 517 961 135 654 457 722 806 424 813 887 058 962 ∴
  135 783 606 794 023 527 714 919 218 498 203 673 271 557 355 313 750 622 061 157 577 910 208 832 441 349 389 616 862 561 967 242 177 264 410 366 ∴
  239 051 510 320 517 168 740 669 181 826 271 917 519 330 064 397 334 253 279 958 891 515 760 991 982 220 699 699 362 514 543,
 98 416 381 192 257 134 121 142 109 574 411 578 161 201 416 302 040 429 474 716 473 622 865 620 556 924 560 470 488 413 446 152 729 066 969 446 ∴
  669 001 319 969 058 278 335 935 545 967 932 612 745 337 153 300 664 140 751 225 265 182 834 444 761 513 699 124 183 110 379 390 699 995 494 745 ∴
  612 500 849 389 129 643 726 072 265 220 344 580 105 128 705 237 768 340 408 615 004 166 701 521 959 638 200 237 677 622 041,
 102 845 913 823 042 325 791 910 452 247 550 664 641 407 894 966 928 790 202 424 691 911 492 603 723 783 956 874 693 603 917 772 223 006 728 362 ∴
  910 985 290 743 642 635 104 457 052 595 098 162 069 447 202 866 777 454 540 421 361 040 039 734 377 931 625 244 913 598 714 833 645 254 395 175 ∴
  148 291 408 692 778 479 703 304 314 254 319 244 525 494 478 277 984 672 139 705 975 919 104 422 577 859 667 637 414 448 755,
 115 727 065 617 801 469 478 314 232 245 392 497 749 284 219 565 250 485 470 168 983 808 914 689 829 169 849 785 211 336 715 953 014 002 523 538 ∴
  613 272 460 097 840 272 045 215 006 966 176 638 317 234 043 694 893 360 961 442 423 085 276 249 527 040 519 912 505 656 686 353 582 019 708 826 ∴
  386 631 739 083 080 864 535 700 390 944 060 831 101 042 908 751 017 702 306 082 839 797 930 786 328 426 533 546 795 505 742}
```

dx1 == m1

```
True
```