EXAMEN ECRIT

CORRECTION

Sans documents

Les calculatrices sont autorisées

Consignes pour l'examen :

Répondez aux questions dans les espaces de réponse prévus dans le sujet.

Indiquez vos nom, prénom et groupe ci-dessous :

NOM

Prénom

Partie I : Arithmétique

Calculer le PGCD de 161 et de 133

L'algorithme d'euclide donne :

a	b	r=a[b]
161	133	28
133	28	21
28	21	7
21	7	0

Le dernier reste non nul vaut 7 : c'est donc le pgcd de 161 et 133 . $pgcd(161,133) = 7$

Calculer le couple de coefficients de Bezout (u, v) tels que $131.u + 74.v = pgcd(131,74)$

Quelle est alors la valeur du pgcd de 131 et 74 ?

L'algorithme d'euclide étendu donne :

r	u	v	q
131	1	0	
74	0	1	1
57	1	-1	1
17	-1	2	3
6	4	-7	2
5	-9	16	1
1	13	-23	5
0	algorithme	terminé	

Le couple (u, v) est alors $(13, -23)$ et le pgcd est égal à 1

Partie II : calculs dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Question 2

On se place dans $(\frac{\mathbb{Z}}{28\mathbb{Z}}, \oplus, \otimes)$.

Calculez les valeurs suivantes :

$$\overline{17} \oplus \overline{23} = \overline{(17+23)[28]} = \overline{40[28]} = \overline{12}$$

$$\overline{17} \otimes \overline{23} = \overline{(17 \times 23)[28]} = \overline{391[28]} = \overline{27}$$

$$\overline{15}^2 = \overline{15} \otimes \overline{15} = \overline{(15 \times 15)[28]} = \overline{225[28]} = \overline{1}$$

A l'aide de l'algorithme d'Euclide étendu, calculez l'inverse de $\overline{9}$

Le tableau d'euclide étendu est le suivant :

r	u	v	q
28	1	0	
9	0	1	3
1	1	-3	9
0			

Ainsi, $1 \times 28 - 3 \times 9 = 1$. Le coefficient -3 associé à 9 étant négatif, on lui ajoute 28 : $28 - 3 \ = \ 25$

Ainsi, $\overline{25}$ est l'inverse de $\overline{9}$

Résoudre les équations suivantes :

$(\overline{15} \otimes x) \oplus \overline{4} = \overline{27}$ étape 1 : on ajoute l'opposé de $\overline{4}$, qui est $\overline{24}$: $\overline{4} \oplus \overline{24} = \overline{0}$

$(\overline{15} \otimes x) \oplus \overline{4} \oplus \overline{24} = \overline{27} \oplus \overline{24} \Rightarrow (\overline{15} \otimes x) = \overline{23}$

étape 2 : on multiplie par $\overline{15}$, car $\overline{15} \otimes \overline{15} = \overline{1}$ (questions précédentes)

$\overline{15} \otimes (\overline{15} \otimes x) = \overline{15} \otimes \overline{23} \Rightarrow x = \overline{9}$

$(\overline{25} \otimes x) \oplus \overline{19} = \overline{6}$ étape 1 : on ajoute l'opposé de $\overline{19}$, qui est $\overline{9}$

$(\overline{25} \otimes x) = \overline{15}$ étape 2 : on multiplie par $\overline{9}$, qui est l'inverse de $\overline{25}$

$x = \overline{23}$

Calculez : $\overline{23}^2, \overline{23}^3, \overline{23}^4, \overline{23}^5, \overline{23}^6$

$\overline{23}^2 = \overline{25}$

$\overline{23}^3 = \overline{15}$

$\overline{23}^4 = \overline{9}$

$\overline{23}^5 = \overline{11}$

$\overline{23}^6 = \overline{1}$

Partie III : applications à la cryptographie

Rappels

$\varphi(n)$ est l'indicateur d'Euler, et indique le nombre d'éléments inversibles dans $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$

Si p est un nombre premier, alors $\varphi(p) = p - 1$

Si p et q sont premiers entre eux, alors $\varphi(p.q) = \varphi(p).\varphi(q)$

Si p est un nombre premier, alors $\varphi(p^k) = (p-1).p^{k-1}$

Calculer les valeurs de $\varphi(n)$ pour :

$n = 37$ 37 est premier, donc $\varphi(37) = 36$

$n = 91$ $91 = 7 \times 13$, 7 et 13 étant premiers entre eux, on a : $\varphi(7.13) = \varphi(7).\varphi(13) = 6.12 = 72$ $\varphi(91) = 72$

$n = 125$ $125 = 5^3$, $\varphi(5^3) = (5-1).5^{3-1} = 4.5^2 = 100$ $\varphi(125) = 100$

$n = 189$ $189 = 3^3 \times 7$, $\varphi(3^3 \times 7) = \varphi(3^3).\varphi(7) = 18 \times 6 = 108$ $\varphi(189) = 108$

Une personne A publie sa clé publique $(n, e) = (91{,}5)$.

A partir de la valeur de $\varphi(n)$, calculez la valeur de sa clé privée d.

On a calculé, dans l'exercice précédent, que $\varphi(91) = 72$. La clé privée d est calculée telle que : $e.d + k.\varphi(n) = 1$, donc : $5.d + k.72 = 1$

L'algorithme d'euclide étendu indique :

r	u	v	q
72	1	0	
5	0	1	14
2	1	-14	2
1	-2	29	2
0			

Donc -$2x72 + 29x5 = 1$. La clé privée d vaut donc 29 $d = 29$

Vous interceptez le message crypté '15' à destination de la personne A. Décryptez ce message en utilisant l'exponentiation rapide.

Pour déchiffrer un message m, il faut calculer $m^d[n]$, avec : $m = 15, d = 29, n = 91$

Soit $15^{29}[91]$ $29 = 16 + 8 + 4 + 1$

$$15^{29}[91] = 15^{16+8+4+1}[91] = 15^{16}[91].15^{8}[91].15^{4}[91].15[91]$$

On construit alors le tableau des puissances de 15 modulo 91

Puissance p	15^p	$15^p[91]$
1	15	15
2	225=15.15	43
4	1849=43.43	29
8	841=29.29	22
16	484=22.22	29

D'où $15^{29}[91] = (29.22.29.15)[91] = 71$

Le message original est 71. Vérification : si on chiffre 71 avec la clé publique $(n = 91, e = 5)$: le message chiffré est $71^5[91] = 15$

Partie III : Protocole RSA

Vous souhaitez recevoir des messages secrets en utilisant le protocole RSA.

A partir de la liste de nombres premiers qui vous est fournie en page suivante, indiquez :

Comment sont choisies/calculées les valeurs des clefs publiques et privées pour RSA

C'est le point que nous avons longuement abordé lors du dernier cours de révision :

Afin de sécuriser le chiffrage/déchiffrage par l'exponentiation modulaire, il faut choisir n comme produit de deux nombres premiers p et q assez grands et proches :
$n = p.q$
Cela permet de calculer $\varphi(n) = (p-1).(q-1)$

Ensuite, on choisit l'exposant e tel que e soit premier avec $\varphi(n)$

En appliquant l'identité de Bezout, on calcule d positif et inférieur à $\varphi(n)$ tel que :
$e.d + k.\varphi(n) = 1$, ou encore $e.d = 1[\varphi(n)]$

(n, e) est alors la clé publique qui sert aux autres personnes à chiffrer
(n, d) est alors la clé privée qui permet de déchiffrer

Faites votre propre choix dans la liste et indiquez :

Votre clef publique : prendre n comme produit de deux des nombres de la liste, prendre e comme un nombre de cette liste (ou être certain qu'il est premier avec $\varphi(n)$)

Votre clef privée : calculer d à partir de e et $\varphi(n)$

Liste de nombres premiers pour RSA

Tous les nombres premiers de 1 à 1000

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
229 233 239 241 251 257 263 269 271 277 281 283 293 307
311 313 317 331 337 347 349 353 359 367 373 379 383 389
397 401 409 419 421 431 433 439 443 449 457 461 463 467
479 487 491 499 503 509 521 523 541 547 557 563 569 571
577 587 593 599 601 607 613 617 619 631 641 643 647 653
659 661 673 677 683 691 701 709 719 727 733 739 743 751
757 761 769 773 787 797 809 811 821 823 827 829 839 853
857 859 863 877 881 883 887 907 911 919 929 937 941 947
953 967 971 977 983 991 997