Elementos de Criptografia
Enunciado do Trabalho Prático
4° Ano LESI/LMCC
2003/2004

Manuel Bernardo Barbosa @ di.uminho.pt

April 14, 2004

Grupo I

Efectue a criptoanálise destes quatro criptogramas que foram obtidos recorrendo a cifras de substituição, Affine e Vigenere. Deve que determinar que cifra foi utilizada em cada um dos casos.

Apresente todo o trabalho que desenvolver, incluindo o código, e explique como chegou a uma solução. Não é suficiente apresentar o texto limpo.

Pistas:

- Os textos limpos são em Português.
- Não contêm acentuação de nenhum tipo, espaços ou pontuação..
- Os valores típicos da análise de frequência aplicáveis em Inglês não são aplicáveis neste caso: terão de ser calculados propositadamente para este efeito.
- Quanto melhor for a qualidade dos valores que obtiver, maiores serão as hipóteses de que os seus palpites estejam correctos.

```
RASEXODCTJPKZSTATGCLGVETXGMGUDFEUAIWEDITTSNVFDRUVGSTIOOK
EOCVKLSUCPQWMHQETGWRGCQVIEEFFOBWROJOEJSFASDSPVEAGFENEKSD
WZTSNAJQCPRVRSTIPHQQMGFBDGMGUAUITRSSUBRFOVGSUVWIEQSGPQRW
UTBWGPSUTBKGNKOATECRWCDBWEADQTBWGMMKTPKTAFFEBUWAFVIEEFEV
GPPRGCWUSBVKAWZIHMTISOIMIFURGNUSUFGIUFXQEKUAUYTNGEIOGQPS
TATITTJCNTTQRLCDBHCTWTRBTCRSOASXGEEGSNSCSKKMPWXEFVOTTQDW
TIBQNENCRPTQDSUCBPQTSUPPPCRWUUNEOAFGISEOEDJOSWGRACASVCNB
CRRYCLIWESWWBKVAOGKAWUCVVCCSRAAHGFSBESGQPACSEIUIHTOQVKAM
OAQISUWPANESUAPAEIGSUWRFGGRIWEDSNOUCRJEOOKGMNETTWGQVIEOE
GCBVKADQGPETEHTOEYBIJUEVXKLABAOHQMSVESMCIKKNEMIEFCSQINAK
EAMSVAKKNUIKRSUETWCSECQVMPAKGXJWVEEEHBQCMGULIIUPDCNUEU
```

```
BHUGLBLLBFHBXBDHNBHYJUGHUSXBUHHSDLBOXKHCKNDNSNAHXCKHSNPHDXUSX
TJHMTJXKOLKDHGXXUXKFNHPAHCHQGXTJXYKHKMNFHPLXBTJNDNPHBCLGXDLBCK
LGJQNKLBDLGJMLBXBBXUPNHNBGHANGHDHBULULBBLKXPNCNXUSXBLSXDLBHBUL
SHBGHDJBNPHANSHMXUHLHCKLCKNHDJBNPHLBDLGJMLBDLMXPJMHKXBGXAXDBXK
HBBLPNHGLBUHBXTJXUPNHPXKSHHANGHXPLDPXKSXQHDHNBGLTJXLBHDNULHPNG
LBTJXPLUBSNSJXDHBCKLSXNUHBXLBUJPMXLSNGLBTJXPLDCLXDLBHPNGLBUJPM
XNPLBDHBHSXULLKGXUHDXUSLGXBSXBDLGJMLBXDMLUFHBPHGXNHBDLMXPJMHKX
BSXDWHANGLBJYBSHUPNHMCKLFKXBBLSXPUNPLXDPLUGNPLXBBXDXMWHUSXBHBG
HSXKKHCKNDNSNAHEHOLKHDHBBLPNHGLBHDNUHPNGLBTJXKXBJMSHKHDXDDLMXP
JMHBHONUBGHBCKLSXNUHBHMFJDHBGHBTJHNBPHCHQXBGXPLUSKLMHKXDYLKHOK
HPHDXUSXKXHPPLXBTJNDNPHBHDHUXNKHGHBXUQNDHB
```

YGEHZNUGWFMIDXSTUOKNVPGLQNIORTENEMDEDNIFJTHURIFEQJVPOICUREFSUXE
UVRHUWFDQKUMTHUULMEVIQMTSVCEHGFSITUWBMOIMEWZSQIHPGLQHIURMUFLPIA
QGIEZDQKYFJELUSBGRERMNRNTIIRLEKGRVDEHIGSVSSYRUVDUXIURLXYWTVVQCH
FJTQWEOUOIYVBFPBURFKAXUFJKATIEQRRJCVEVQKYHJJTQHGJREFIWTZVUFWBSE
BIWFVXYMXFDSULITZNJYPJXEDNITKABPITKEDBENTODMXSLITIITKRKNYSRSGOI
QFSIOENTOCJSOVNJYWEVABNSDFNJLETKEDOQBVSSUPBUELUVJFSGOMMFMUNVPJE
INVVKUHUWEVTUWXBMEYMUVRNTISTEOIMSTJIININRSEJXJTOIYEEZSJURDZATUX
FIRQJVPGOHWMPEAHYQVDAHYWPCUSUSEVQKCPPDEJLSTEOUHXBETEUITKATCWURN
SCEBKEHLEQRRUWIUFTQFQFETUUVJUADUSIRSYHEJJDUPMERIDNIMZGUHXFFUEOX
SRECFSDRIIUUVVCXUQBDOIHSWRIELUVVBEMXPEMEMGPMOBIREIEIJESZSRYVMZM
JIUVZOUJIRLICMIIRSULITZNJYPJXEDNITEAJYVSRNQIQPCDQLENRPQCWBXECUJ
PIMQMKFFMUNVJTAILIHLLQLITRUCUVFJOBOGBFDUOQRLIBIQFKRE

PAIGSSYHMYAYKYIMSWIPAFSGUNZWUPAHYAAYGIYPHGWHMYSWGSUYJYMPK
KWDNWUGAPGFSGBPBYKJYHMYPTGHMYUGWJYHAGIPJFGJPRHYMWIGUYQNFW
MYSGJPWGSYJMGUGGAWAMYJPAGKPSYUPIWHMNSPUYYKYIMSGYAYUYFSGMG
YADNYKEYYAMPPAAGIWPUPYAMPAFPSMWINKPAIPSSYRPUPAFSGQYIMPUPA
UGAGKYBPSSWUPAYJAYRNWUPFYKGBYHMGAGKPSAPGYHMPGIPFMNSPUPAFY
KGIPJFGJPRHYMWIGUYQNFWMYSNJPRSPHUYFPSMYUYKPAAPGPFSWAWGHPU
PAPNJPPKMWMNUYJNWMGANFYSWGSPUPAHNBYHATWIPHUGIGHUYHPUPAPSW
IGIEYMYPSUYNJFGKGPGGNMSGPMYYHIGHMSPSYJFGSPIPAGNJPJGKYINKP
PMJGATYSWIPUYPKMPPKMWMNUYYAYSYJSYJGBWUPAUPIWHMNSPUYSPUWPI
PGWGUYAKGIPAYHNJPGSOWMPMPGFSGCWJPUYQNFWMYSDNYSPARPKWMYSPK
JYHMYYAAPWJYHAPSPUWPIPGISWPHUGIPAIPMPAUYFPSMWINKPAIPSSYRP
UPAPADNPWAFGSANPBYZGSWRWHPJBWGKYHMPAYCFKGAGYAUYYHYSRWPSPU
WG

Grupo II

1. Calcule os seguintes valores utilizando o algoritmo de Euclides:
   - $mdc(4653, 9337)$
   - $4653^{-1} \pmod{9337}$
   - $mdc(8763, 8771)$
   - $8763^{-1} \pmod{8771}$
2. Resolva o seguinte sistema de congruências:
   $$\begin{cases} x \equiv 33 \pmod{41} \\ x \equiv 74 \pmod{83} \\ x \equiv 86 \pmod{91} \end{cases}$$
3. Resolva o seguinte sistema de congruências:
   $$\begin{cases} 21x \equiv 72 \pmod{89} \\ 62x \equiv 98 \pmod{111} \end{cases}$$

Grupo III

Utilizando a técnica RSA foram obtidos os seguintes criptogramas. Os parâmetros públicos utilizados foram $n = 18221$ e $\beta = 8557$, no primeiro caso, e $n = 30621$ e $\beta = 16363$, no segundo caso. "Quebre" estas cifras, tendo em conta que, devido à dimensão de n nos dois casos, o problema da factorização do módulo é relativamente fácil de resolver. Tenha ainda em consideração os seguintes pontos:

- Para recuperar o texto limpo necessita de saber como foi codificado. Neste caso, cada letra é tratada como um elemento de $\mathbb{Z}_{26}$, e cada trio de letras $L_1L_2L_3$ é codificado num número $L_1 * 26^2 + L_2 * 26 + L_3$.
- Escreva e use os seus próprios programas para desempenhar esta tarefa.
- Submeta listagens comentadas das partes relevantes do código que produzir, o texto limpo que recuperou e uma explicação de como procedeu para resolver o problema.

12120	7872	5374	11172	16639	17767	11420	16765	15249
7979	17678	17623	14756	9567	5715	17541	9867	752
10724	13411	5480	11010	1369	6016	15499	2004	3451
6869	8610	12807	1897	18185	17209	2011	3343	5315
8916	10724	13411	5480	11010	2071	1864	8255	3200
17476	5875	13985	9189	8181	4697	14668	10208	16919
13907	8916	14288	5190	16345	11203	11230	5307	17767
11420	16765	2434	7853	9030	14386	8239	2141	17953
12519	11438	1113	13985	905	11709	5578	8916	7425
4196	15176	10377	15361	468	9850	17798	10079	16693
16759	13003	9718	5818	10624	8610	5000	14742	10385
9274	3615	11283	10282	6506	327	8934	12713	9940
12502	994	3521	16553	12361	17415	450	9989	5126
13779	4768	12604	7548	14542	12339	16250	6935	2666
14875	16765	17531	2489	11240	2573	2489	14151	8916
4768	6506	863	9926	12819	2638	2058	5048	4304
13239	15359	18100	4768	14893	17699	6079	5770	11507
2560	3875	9747	3518	10724	13411	5480	11010	

4106	29137	29135	1180	7630	2568	4497	29664	18473
13368	17272	8364	10156	16467	12138	23219	12642	22008
23720	12643	5123	17575	27277	17177	21783	10443	7642
5123	17575	16955	12138	23219	17809	23473	13676	25180
11504	28622	1088	12073	25869	29664	10517	15348	1479
21662	26773	6953	28110	1141	22356	16573	16955	15371
16573	24792	24249	8391	26188	14970	2695	8276	23235
8276	18999	21661	22742	18755	15101	6183	28622	21997
901	15947	8991	19452	23383	18510	30334	15101	19773
3447	11475	30271	14597	4106	23473	23473	8467	17781
8391	25919	13570	24620	26623	7489	24257	20044	22742
18755	11504	962	6323	23613	24792	3979	28926	25838
23613	2040	12941	25665	8272	4903	29989	24604	10782
322	1746	22532	662	14671	13894	23614	16028	20974
27617	15768	26647	28073	7676	13903	29664	3766	8654
21578	4325	4886	7676	8893	299	25838	10756	13026
6263	243	21770	3149	19164	22008	20977	19727	26075
24519	15864	16955	1141	14597	29272	24128	14512	9642
24519	15864							

Grupo IV

1. Escreva um programa para calcular símbolos de Jacobi utilizando as seguintes propriedades.

   (a) Se n é um inteiro impar, e $m_1 \equiv m_2 \pmod{n}$, então $\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right)$.

   (b) Se n é um inteiro impar, então
   $$\left(\frac{2}{n}\right) = \begin{cases} 1 & se\ n \equiv \pm 1 \pmod 8 \\ -1 & se\ n \equiv \pm 3 \pmod 8 \end{cases}.$$

   (c) Se n é um inteiro impar, então
   $\left(\frac{m_1 m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right)$
   e, em particular, se $m = 2^k * t$
   $\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^k \left(\frac{t}{n}\right)$.

   (d) Se m e n são inteiros impares, então
   $$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & se\ m \equiv n \equiv 3 \pmod 4 \\ \left(\frac{n}{m}\right) & nos\ restantes\ casos \end{cases}.$$

   O programa não deverá fazer factorização mais complexa do que a divisão por potências de 2.

2. Teste o programa que desenvolveu para a alínea anterior, calculando: $\left(\frac{782}{893}\right)$, $\left(\frac{43298}{2389}\right)$ e $\left(\frac{762534}{93939393}\right)$.

3. Para n = 761, 937 e 1813 encontre as bases b, para as quais n é um pseudo-primo de Euler. (Nota: n é um pseudo-primo de Euler na base b se o símbolo de Jacobi $\left(\frac{b}{n}\right)$ é igual a $b^{(n-1)/2} \pmod n$.)

4. Retire conclusões quanto à utilidade do símbolo de Jacobi num teste de primalidade, relacionando com um método que tenha estudado nas aulas teóricas.

Grupo V

1. "Quebre" este criptograma sabendo ele foi obtido com uma cifra El Gamal. Os parâmetros do sistema são $N = 51347 = 1 + 2 * 25673$ (51347 e 25673 são primos), $\beta = 42857$ e $g = 2$. Repare que, devido à dimensão do módulo, a resolução do Problema do Logaritmo Discreto e a inversão da chave pública torna-se practicável.

(5849,29399)	(32536,17952)	(5534,20712)	(20600,30764)
(12814,17043)	(11507,13817)	(11881,20855)	(4846,17737)
(25479,29226)	(2605,3645)	(2296,16849)	(9431,32649)
(28292,18380)	(26329,27119)	(24960,14581)	(16389,6576)
(28143,17337)	(26045,7909)	(15512,24206)	(11967,3466)
(18293,14683)	(28252,41776)	(9915,36143)	(4939,40126)
(4751,39677)	(16202,31341)	(1419,33556)	(30171,18869)
(39126,32387)	(28857,20284)	(18692,3715)	(10793,30585)
(4574,35261)	(31924,11641)	(20129,38975)	(38118,33840)
(7251,2859)	(17616,16822)	(36750,36085)	(37234,27675)
(1419,11592)	(17070,17924)	(19763,14920)	(19066,1553)
(16288,22006)	(10763,33352)	(26825,36887)	(4895,29503)
(39330,15222)	(11199,5216)	(41930,13466)	(14584,19048)
(23649,19434)	(404,2931)	(34841,9129)	(34191,37750)
(37234,1993)	(6886,30271)	(32105,2333)	(19619,42692)
(12355,28273)	(39929,42479)	(23685,18389)	(41561,1835)
(31905,35969)	(37919,38943)	(12527,40801)	(13026,39940)
(8049,36750)	(841,39959)	(33771,36698)	(18658,9622)
(11732,41610)	(8458,34114)	(4945,22898)	(38252,18896)
(24710,35233)	(26273,8147)	(5742,7585)	(17064,41944)
(22082,30912)	(8417,31072)	(1463,3056)	(21858,17581)
(3472,8014)	(15301,15755)	(26250,34244)	(23464,2693)
(36750,39616)	(395,4217)	(27641,1616)	(6342,14121)
(13888,31076)	(16386,41227)	(37069,1950)	(41301,22958)
(40853,14711)	(36559,14990)	(10558,31722)	(12397,30676)
(28331,27145)	(30211,7049)	(36707,35760)	(2857,12890)
(25397,20273)	(27182,18585)	(32053,23460)	(17797,29063)
(6513,21407)	(13120,36211)	(29530,41987)	(11358,28908)
(7172,24617)	(5965,7302)	(15988,31700)	(41513,16267)
(17084,17411)	(7852,-40387)	(30191,9375)	(17627,1999)
(26261,33158)	(529,770)	(3935,17081)	(9983,3981)
(24852,21606)	(9643,25028)	(24479,31720)	(32517,31294)
(25198,13183)	(24710,35022)	(40376,33264)	(34944,27487)
(7136,5400)	(17593,527)		

- A codificação de caracteres é idêntica à do exercício III-3.
- Escreva e use os seus próprios programas para desempenhar esta tarefa.

- Submeta listagens comentadas das partes relevantes do código que produzir, o texto limpo que recuperou e uma explicação de como procedeu para resolver o problema.

2. Quais são os valores secretos do parâmetro k utilizados na cifragem da alínea anterior? Utilize o algoritmo de Shank para encontrar os 20 primeiros valores. Note que estes valores não são necessários para a decifragem. O que se pretende neste exemplo é demonstrar o funcionamento dos algoritmos de resolução do problema do logaritmo discreto.

Grupo VI

1. Determine quais dos seguintes polinómios são irredutíveis em $\mathbb{Z}_2[x]$: $x^5 + x^4 + x^2 + 1$, $x^5 + x^2 + 1$, $x^5 + x^4 + x^3 + x^2 + 1$.

2. O corpo $GF(2^5)$ pode ser construído como $\mathbb{Z}_2[x]/(x^5 + x^3 + 1)$. Calcule neste corpo:

   (a) $(x^3+x^2)*(x^4+x^2+1)$ e $(x^5+x)^{-1}$ utilizando uma versão generalizada do algoritmo de Euclides.

   (b) $(x^3 + 1)^{34}$ utilizando uma versão generalizada do algoritmo de exponenciação binária.

3. Considere a curva elíptica $y^2 = x^3 + 13x + 37$ definida sobre $\mathbb{Z}_{107}$. Escreva um programa para:

   (a) Calcular o número de pontos em E.

   (b) Determinar a ordem máxima de um elemento em E e encontrar um elemento com essa ordem.

   (c) Determinar se E é cíclico.

References

[1] Douglas R. Stinson. *Cryptography - Theory and Practice*. CRC Press, 1995.