

CSCI 284 - Cryptography - Spring 2008
George Washington University

Homework V: due before final exam, 12 May, 2008

This is an extra credit HW. It is worth a 100 points, and can be used to substitute your worst 100 point performance in the HWs. That is, it can be used to substitute all of HWs 1 or 2 and 25 points of another HW, or all of HW 3, or 4/5 of HW 4.

Policy on collaboration: All examinations, papers, and other graded work products and assignments are to be completed in conformance with The George Washington University Code of Academic Integrity. You may discuss HWs among yourselves, and work on them in groups. However, each student is expected to write his or her own HW out independently; you may not copy one another's assignments, even in part. You may not collaborate with others on the quizzes, midterm, or final.

You are expected to cite all your sources in any written work that is not closed book. Sources may be papers, books, web sites, discussions with others - faculty, friends, students. For example, if, in a group, one student has a major idea that leads to a solution to a HW problem, all other students in the group should cite this student.

Any violations will be treated as violations of the Code of Academic Integrity.

PLEASE submit all HW on Blackboard only. Name your report:
CS284_HW5_LASTNAME_FIRSTNAME.doc or .pdf.

Archive the code with the report and name the compressed file similarly, with extensions .tar or .rar or .zip

All code must run on your hobbes account. The TA will make no attempt to debug your code, or determine why it does not run. You will be graded on the correctness of your output, the quality of your code: efficiency and documentation, and the quality of your report. There will be no exceptions.

On no account may you use code written by anyone else, whether you acknowledge it or not.

This problem is from the text.

Two samples of RSA ciphertext are presented in the attached Tables 4.1 and 4.2. Your task is to decrypt them. The public parameters of the system are $n = 18923$ and $b = 1261$ (for Table 4.1) and $n = 31313$ and $b = 4913$ (for Table 4.2).

The decryption may be accomplished as follows First, factor n (which is easy; it is small). Then compute a by first determining $\phi(n)$. Finally, decrypt the ciphertext. Use efficient exponentiation.

The numbers you obtain may be converted to the English alphabet. Three letters in the English alphabet are converted to numbers as follows: if the three letters are represented by numbers abc (for example, DOG is represented by 3 14 6), this corresponds to the value $a \times 26^2 + b \times 26 + c$; thus DOG corresponds to 2398, CAT to 1371 and ZZZ to 17575. You have to invert this process for your final step; that is, given the results of RSA decryption, convert each value to a base 26 representation, which is straightforward to convert to the alphabet.

You should submit a report that describes what you did and the solutions you obtained, as well as all your code.

TABLE 4.1
RSA Ciphertext

12423	11524	7243	7459	14303	6127	10964	16399
9792	13629	14407	18817	18830	13556	3159	16647
5300	13951	81	8986	8007	13167	10022	17213
2264	961	17459	4101	2999	14569	17183	15827
12693	9553	18194	3830	2664	13998	12501	18873
12161	13071	16900	7233	8270	17086	9792	14266
13236	5300	13951	8850	12129	6091	18110	3332
15061	12347	7817	7946	11675	13924	13892	18031
2620	6276	8500	201	8850	11178	16477	10161
3533	13842	7537	12259	18110	44	2364	15570
3460	9886	8687	4481	11231	7547	11383	17910
12867	13203	5102	4742	5053	15407	2976	9330
12192	56	2471	15334	841	13995	17592	13297
2430	9741	11675	424	6686	738	13874	8168
7913	6246	14301	1144	9056	15967	7328	13203
796	195	9872	16979	15404	14130	9105	2001
9792	14251	1498	11296	1105	4502	16979	1105
56	4118	11302	5988	3363	15827	6928	4191
4277	10617	874	13211	11821	3090	18110	44
2364	15570	3460	9886	9988	3798	1158	9872
16979	15404	6127	9872	3652	14838	7437	2540
1367	2512	14407	5053	1521	297	10935	17137
2186	9433	13293	7555	13618	13000	6490	5310
18676	4782	11374	446	4165	11634	3846	14611
2364	6789	11634	4493	4063	4576	17955	7965
11748	14616	11453	17666	925	56	4118	18031
9522	14838	7437	3880	11476	8305	5102	2999
18628	14326	9175	9061	650	18110	8720	15404
2951	722	15334	841	15610	2443	11056	2186

Exercises

159

TABLE 4.2
RSA Ciphertext

6340	8309	14010	8936	27358	25023	16481	25809
23614	7135	24996	30590	27570	26486	30388	9395
27584	14999	4517	12146	29421	26439	1606	17881
25774	7647	23901	7372	25774	18436	12056	13547
7908	8635	2149	1908	22076	7372	8686	1304
4082	11803	5314	107	7359	22470	7372	22827
15698	30317	4685	14696	30388	8671	29956	15705
1417	26905	25809	28347	26277	7897	20240	21519
12437	1108	27106	18743	24144	10685	25234	30155
23005	8267	9917	7994	9694	2149	10042	27705
15930	29748	8635	23645	11738	24591	20240	27212
27486	9741	2149	29329	2149	5501	14015	30155
18154	22319	27705	20321	23254	13624	3249	5443
2149	16975	16087	14600	27705	19386	7325	26277
19554	23614	7553	4734	8091	23973	14015	107
3183	17347	25234	4595	21498	6360	19837	8463
6000	31280	29413	2066	369	23204	8425	7792
25973	4477	30989					

a message to Bob by representing each alphabetic character as an integer between 0 and 25 (i.e., $A \leftrightarrow 0, B \leftrightarrow 1$, etc.), and then encrypting each residue modulo 26 as a separate plaintext character.

- (a) Describe how Oscar can easily decrypt a message which is encrypted in this way.

(b) Suppose that Oscar intercepts the following ciphertext (which was an