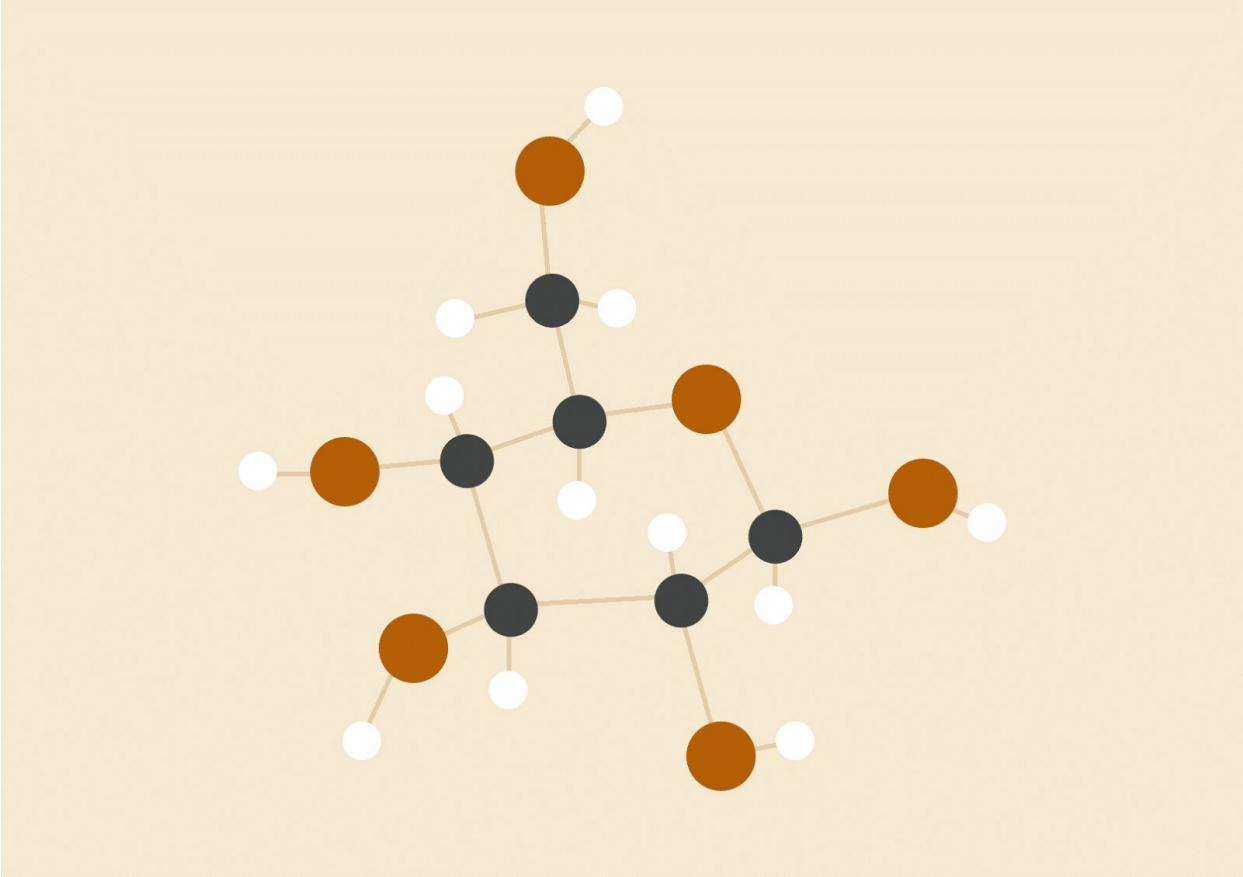
Group G

Cryptography Report

A report on our cipher



[redacted]

09.010.2015

Math 485 - Cryptography

INTRODUCTION

We were presented with the problem of keeping communications secure between the OCRA Creative Recursive Acronyms, Inc. We were asked to create a cryptosystem, and likewise an encryption key, for the engineers at OCRAI to create a mobile application to encrypt text communication. The requirements for our cryptosystem stated that given a plaintext of standard text message size, the ciphertext must be between 500 to 700 characters. In addition, the ciphertext should be able to be typed on a standard keyboard. We were also asked that the encryption key be no longer than 10 letters long, should the key be using a sequence of letters; the reason behind this is that it would slow down the processing power of the application.

OUR CRYPTOSYSTEM - THE PROCESS OF OBTAINMENT AND HOW IT WORKS

Our hope for our cryptosystem was that it would be one that we would find secure and reliable. We were trying to find a cryptosystem that would take some time to decrypt, but wouldn't be too overbearing for the application's processing power. We were also hoping to create a system where the key could be manipulated and not very predictable, thereby creating a complex manner in which to encode a message.

We first considered ways to use a sequence of letters as our key. This design involved assigning a unique sequence of five letters to each letter of the alphabet. The concern we had with this method was that the assignment was very predictable and difficult to randomize, and thus unable to securely protect the messages. Likewise, it did not allow for a wide variety of encryption keys, which meant that if the key was discovered, there would a limited amount of keys to try before every key would be broken.

We also considered a method that involved taking an irrational number and assigning the values of each digit placement to a unique letter in the alphabet. However, as we tried this method, we realized that we found ourselves in a similar situation to our first method; the number of possible numerical values that we could truly use would limit the amount of encryption keys. We also realized that this method would be very difficult to manipulate, defeating one of the purposes we were aiming to achieve.

Another method we had considered was using a displacement key. This particular method would allow for better manipulation. As we experimented with this method, we realized that by using a displacement key, the amount of time it would take to

encrypt or decrypt a short message was more than intended for the purposes of this particular project. The reason behind this is based on the fact that this particular method requires the decryptor to test every possible displacement for consistencies. This method would create a very secure key; however, as already stated, it would be outside the parameters of what this particular assignment entailed.

After the above attempts, we decided to use a cryptosystem that uses random digit tables to encrypt and decrypt our codes. The idea behind us using a random digit table was that it had the potential to securely encrypt data and the messages we would send. The use of a random digit table for our cryptosystem follows a simple process. On the left hand side of the random digit table, like the one we have attached to the end of this particular report, is a column titled lines. We would choose a line, and then select an entry. Depending on the digit table, there will be more entries per line or fewer. Our example table, as you will notice, contains eight entries per line. After selecting a line and an entry on that line, the encryptor would begin to assign a plaintext letter to each unique five digit value, starting with *a*. The next unique five digit value would be assigned to *b*, the next to *c*, and so forth until the whole alphabet was covered. This method we are describing involves reading from left to right, starting on the selected row and entry. The key will totally depend on which row was used and which entry it starts on. Especially with unique random digit tables, this method can prove to be a bit of a challenge.

CONCLUSION

In summary, we solved the problem of secure text communication by use of a random digit table to generate an encryption key. This method satisfies the ciphertext character limit, in addition to producing multiple encryption keys simply by choosing a new line on the table or by generating a completely different table. The application design should be able to select a line on a random digit table, and assign unique five digit values to each letter in the alphabet, starting with *a*. In the decryption of the text, the same line used to encrypt the message should be used. In utilizing our design to create the mobile application, we encourage the engineers to code and program the generation of various random digit tables to heighten the security of text communication. The reason of this would be to have unique random digit tables built into the programming, ensuring that tables will remain private to the company not for the public use.

87136433675589233063622245602795052545804184255892558924336787136148635458
07518655892290779576147052871364184256027470526222456027558922907756027622
24558928159854580710359505295761138734184281507290777518675186545808186862
22456027751865458095761470525458095761751866222429077470529505295761138735
58928159862224560277518654580616837359229077957614705290908545808159895761
33063545802907755892622246168356027622243306361683815989505295761622245589
26222461683560279505287136622245589243367957614705295052616832907733063622
24616832907775186751866222447052148637518629077616837359275186545803306341
84255892

12975945910036002428555888194043563130489676700360003609459112975335861304
85171900360477811325806928129759676781940069285558881940003604778181940555
88003604109813048238224356313258707089676745144477815171951719130483596300
36081940517191304813258069281304813258517195558847781069284356313258707080
03604109855588819405171913048791774839447781132580692856934130484109813258
12428130484778100360555887917781940555880242879177410984356313258555880036
05558879177819404356312975555880036094591132580692843563791774778102428555
88791774778151719517195558806928335865171947781791774839451719130480
24289676700360

33906845686349494165465148750384568063401005671379264115719597762977620634
08596897762063408750345984100569281306340465146349446514875037655097762928
13054819429294165845685719557195977629483185968465149483185968264117137963
49446514370330548110056713794221184568054816349494165977624221192813465149
42929776246514634949429284568948312641197762977625083063494928139776233906
97762571950548192813977624598484568928130634046514948318596810056713799281
38596810056845685719584568875036349497762845689429294165977629281387503465
14875036349410056941659776257195422111005663494941659776292813875038750397
76297762634949416597762928139776245984845689281306340

TABLE B

Random digits

Line								
101	19223	95034	05756	28713	96409	12531	42544	82853
102	73676	47150	99400	01927	27754	42648	82425	36290
103	45467	71709	77558	00095	32863	29485	82226	90056
104	52711	38889	93074	60227	40011	85848	48767	52573
105	95592	94007	69971	91481	60779	53791	17297	59335
106	68417	35013	15529	72765	85089	57067	50211	47487
107	82739	57890	20807	47511	81676	55300	94383	14893
108	60940	72024	17868	24943	61790	90656	87964	18883
109	36009	19365	15412	39638	85453	46816	83485	41979
110	38448	48789	18338	24697	39364	42006	76688	08708
111	81486	69487	60513	09297	00412	71238	27649	39950
112	59636	88804	04634	71197	19352	73089	84898	45785
113	62568	70206	40325	03699	71080	22553	11486	11776
114	45149	32992	75730	66280	03819	56202	02938	70915
115	61041	77684	94322	24709	73698	14526	31893	32592
116	14459	26056	31424	80371	65103	62253	50490	61181
117	38167	98532	62183	70632	23417	26185	41448	75532
118	73190	32533	04470	29669	84407	90785	65956	86382
119	95857	07118	87664	92099	58806	66979	98624	84826
120	35476	55972	39421	65850	04266	35435	43742	11937
121	71487	09984	29077	14863	61683	47052	62224	51025
122	13873	81598	95052	90908	73592	75186	87136	95761
123	54580	81507	27102	56027	55892	33063	41842	81868
124	71035	09001	43367	49497	72719	96758	27611	91596
125	96746	12149	37823	71868	18442	35119	62103	39244
126	96927	19931	36089	74192	77567	88741	48409	41903
127	43909	99477	25330	64359	40085	16925	85117	36071
128	15689	14227	06565	14374	13352	49367	81982	87209
129	36759	58984	68288	22913	18638	54303	00795	08727
130	69051	64817	87174	09517	84534	06489	87201	97245
131	05007	16632	81194	14873	04197	85576	45195	96565
132	68732	55259	84292	08796	43165	93739	31685	97150
133	45740	41807	65561	33302	07051	93623	18132	09547
134	27816	78416	18329	21337	35213	37741	04312	68508
135	66925	55658	39100	78458	11206	19876	87151	31260
136	08421	44753	77377	28744	75592	08563	79140	92454
137	53645	66812	61421	47836	12609	15373	98481	14592
138	66831	68908	40772	21558	47781	33586	79177	06928
139	55588	99404	70708	41098	43563	56934	48394	51719
140	12975	13258	13048	45144	72321	81940	00360	02428
141	96767	35964	23822	96012	94591	65194	50842	53372
142	72829	50232	97892	63408	77919	44575	24870	04178
143	88565	42628	17797	49376	61762	16953	88604	12724
144	62964	88145	83083	69453	46109	59505	69680	00900
145	19687	12633	57857	95806	09931	02150	43163	58636
146	37609	59057	66967	83401	60705	02384	90597	93600
147	54973	86278	88737	74351	47500	84552	19909	67181
148	00694	05977	19664	65441	20903	62371	22725	53340
149	71546	05233	53946	68743	72460	27601	45403	88692
150	07511	88915	41267	16853	84569	79367	32337	03316

TABLE B

Random digits (continued)

Line								
151	03802	29341	29264	80198	12371	13121	54969	43912
152	77320	35030	77519	41109	98296	18984	60869	12349
153	07886	56866	39648	69290	03600	05376	58958	22720
154	87065	74133	21117	70595	22791	67306	28420	52067
155	42090	09628	54035	93879	98441	04606	27381	82637
156	55494	67690	88131	81800	11188	28552	25752	21953
157	16698	30406	96587	65985	07165	50148	16201	86792
158	16297	07626	68683	45335	34377	72941	41764	77038
159	22897	17467	17638	70043	36243	13008	83993	22869
160	98163	45944	34210	64158	76971	27689	82926	75957
161	43400	25831	06283	22138	16043	15706	73345	26238
162	97341	46254	88153	62336	21112	35574	99271	45297
163	64578	67197	28310	90341	37531	63890	52630	76315
164	11022	79124	49525	63078	17229	32165	01343	21394
165	81232	43939	23840	05995	84589	06788	76358	26622
166	36843	84798	51167	44728	20554	55538	27647	32708
167	84329	80081	69516	78934	14293	92478	16479	26974
168	27788	85789	41592	74472	96773	27090	24954	41474
169	99224	00850	43737	75202	44753	63236	14260	73686
170	38075	73239	52555	46342	13365	02182	30443	53229
171	87368	49451	55771	48343	51236	18522	73670	23212
172	40512	00681	44282	47178	08139	78693	34715	75606
173	81636	57578	54286	27216	58758	80358	84115	84568
174	26411	94292	06340	97762	37033	85968	94165	46514
175	80011	09937	57195	33906	94831	10056	42211	65491
176	92813	87503	63494	71379	76550	45984	05481	50830
177	70348	72871	63419	57363	29685	43090	18763	31714
178	24005	52114	26224	39078	80798	15220	43186	00976
179	85063	55810	10470	08029	30025	29734	61181	72090
180	11532	73186	92541	06915	72954	10167	12142	26492
181	59618	03914	05208	84088	20426	39004	84582	87317
182	92965	50837	39921	84661	82514	81899	24565	60874
183	85116	27684	14597	85747	01596	25889	41998	15635
184	15106	10411	90221	49377	44369	28185	80959	76355
185	03638	31589	07871	25792	85823	55400	56026	12193
186	97971	48932	45792	63993	95635	28753	46069	84635
187	49345	18305	76213	82390	77412	97401	50650	71755
188	87370	88099	89695	87633	76987	85503	26257	51736
189	88296	95670	74932	65317	93848	43988	47597	83044
190	79485	92200	99401	54473	34336	82786	05457	60343
191	40830	24979	23333	37619	56227	95941	59494	86539
192	32006	76302	81221	00693	95197	75044	46596	11628
193	37569	85187	44692	50706	53161	69027	88389	60313
194	56680	79003	23361	67094	15019	63261	24543	52884
195	05172	08100	22316	54495	60005	29532	18433	18057
196	74782	27005	03894	98038	20627	40307	47317	92759
197	85288	93264	61409	03404	09649	55937	60843	66167
198	68309	12060	14762	58002	03716	81968	57934	32624
199	26461	88346	52430	60906	74216	96263	69296	90107
200	42672	67680	42376	95023	82744	03971	96560	55148