Breaking a substitution code	Season	03
	Episode	12
	Time frame	2 periods

Objectives :

- Study the main methods to break a substitution code.

Materials :

- *Excerpt from* The Gold Bug *and tips for frequency analysis.*
- *Beamer.*
- *Texts to decipher.*

1 – Breaking the Gold Bug cipher 55 mins

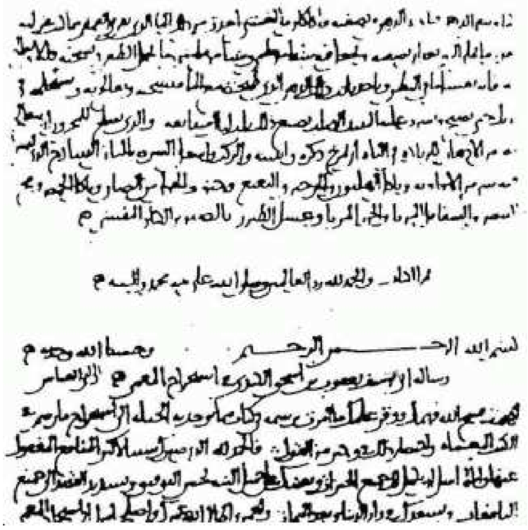
The method is explained by reading the relevant part in *The Gold Bug*, by Edgar Allan Poe. Other tricks are extracted for *The Code Book*, by Simon Singh.

2 – Break a cipher on your own 55 mins

Working in teams, students have to break a substitution code on a short text.

Breaking a substitution code	Season Episode Document	03 12 Document

Although it is not known who first realized that the variation in the frequencies of letters could be exploited in order to break ciphers, the earliest known description of the technique is by the 9th century scientist Abu Yusuf Ya 'qub ibn Is-haq ibn as-Sabbah ibn 'omran ibn Ismail al-Kindi. Known as the philosopher of the Arabs', al-Kindi was the author of 290 books on medicine, astronomy, mathematics, linguistics and music, but his greatest treatise, which was only rediscovered in 1987 in the Sulaimaniyyah Ottoman Archive in Istanbul, is entitled "A Manuscript on Deciphering Cryptographic Messages."



The first page of al-Kindi's manuscript

"The Gold-Bug" is a short story by Edgar Allan Poe, set on Sullivan's Island, South Carolina involving deciphering a secret message and finding buried treasure. The story was first published in the Philadelphia Dollar Newspaper in June 1843 after Poe had won a competition held by the paper, receiving a prize of US100. It includes a detailed description of a method for solving a simple substitution cipher using letter frequencies.

Excerpt from *The Gold Bug* by Edgar Allan Poe

"You observe there are no divisions between the words. Had there been divisions the task would have been comparatively easy. In such cases I should have commenced with a collation and analysis of the shorter words, and, had a word of a single letter occurred, as is most likely (a or I, for example), I should have considered the solution as assured. But, there being no division, my first step was to ascertain the predominant letters, as well as the least frequent. Counting all, I constructed a table thus :

8	;	4	‡	)	∗	5	6	†	1	0	9	2	:	3	?	$	–	.
33	26	19	16	16	13	12	11	8	8	6	5	5	4	4	3	2	1	1

"Now, in English, the letter which most frequently occurs is e. Afterward, the succession runs thus : a o i d h n r s t u y c f g l m w b k p q x z. E predominates so remarkably, that an individual sentence of any length is rarely seen, in which it is not the prevailing character.

"Here, then, we have, in the very beginning, the groundwork for something more than a mere guess. The general use which may be made of the table is obvious – but, in this particular cipher, we shall only very partially require its aid. As our predominant character is 8, we will commence by assuming it as the e of the natural alphabet. To verify the supposition, let us observe it the 8 be seen often in couples – for e is doubled with great frequency in English – in such words, for example, as 'meet,' 'fleet,' 'speed,' 'seen,' 'been,' 'agree,' etc. In the present instance we see it doubled no less than five times, although the cryptograph is brief.

"Let us assume 8, then, as e. Now, of all words in the language, 'the' is most usual ; let us see, therefore, whether there are not repetitions of any three characters, in the same order of collocation, the last of them being 8. If we discover a repetition of such letters, so arranged, they will most probably represent the word 'the.' Upon inspection, we find no less than seven such arrangements, the characters being ;48. We may, therefore, assume that ; represents t, 4 represents h, and 8 represents e – the last being now well confirmed. Thus a great step has been taken. "But, having established a single word, we are enabled to establish a vastly important point ; that is to say, several commencements and terminations of other words. Let us refer, for example, to the last instance but one, in which the combination ;48 occurs – not far from the end of the cipher. We know that the ; immediately ensuing is the commencement of a word, and, of the six characters succeeding this 'the,' we are cognizant of no less than five. Let us set these characters down, thus, by the letters we know them to represent, leaving a space for the unknown – t.eeth.

"Here we are enabled, at once, to discard the 'th,' as forming no portion of the word commencing with the first t ; since, by experiment of the entire alphabet for a letter adapted to the vacancy, we perceive that no word can be formed of which this th can be a part. We are thus narrowed into t.ee, and, going through the alphabet, if necessary, as before, we arrive at the word 'tree,' as the sole possible reading. We thus gain another letter, r, represented by (, with the words 'the tree' in juxtaposition.

"Looking beyond these words, for a short distance, we again see the combination ;48, and employ it by way of termination to what immediately precedes. We have thus this arrangement :

the tree ;4(‡ ?34 the,

or substituting the natural letters, where known, it reads thus :

the tree thr‡ ?3h the,

"Now, if, in place of the unknown characters, we leave blank spaces, or substitute dots, we read thus : the tree thr...h the, when the word 'through' makes itself evident at once. But this discovery gives us three new letters, o, u, and g, represented by and 3.

"Looking now, narrowly, through the cipher for combinations of known characters, we find, not very far from the beginning, this arrangement, 83(88, or egree, which, plainly, is the conclusion of the word 'degree,' and gives us another letter, d, represented by †.

"Four letters beyond the word 'degree,' we perceive the combination ;46(;88.

"Translating the known characters, and representing the unknown by dots, as before, we read thus : th.rtee, an arrangement immediately suggestive of the word 'thirteen,' and again furnishing us with two new characters, i and n, represented by 6 and *.

"Referring, now, to the beginning of the cryptograph, we find the combination, 53‡‡†.

"Translating as before, we obtain .good, which assures us that the first letter is A, and that the first two words are 'A good.'

"It is now time that we arrange our key, as far as discovered, in a tabular form, to avoid confusion. It will stand thus :

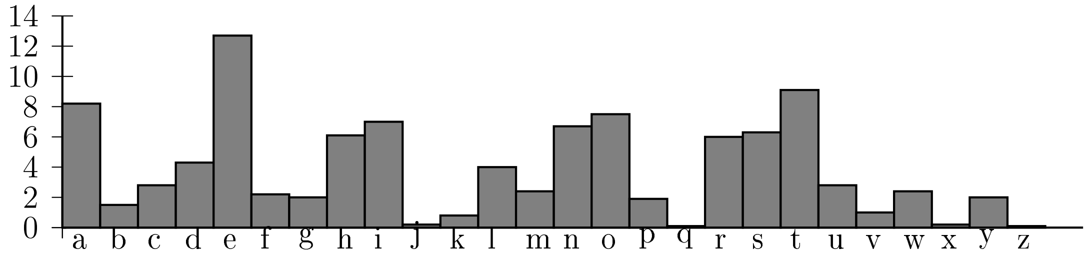
5	represents	a
†	”	d
8	”	e
3	”	g
4	”	h
6	”	i
*	”	n
‡	”	o
(	”	(
;	”	t
?	”	u

“We have, therefore, no less than eleven of the most important letters represented, and it will be unnecessary to proceed with the details of the solution. I have said enough to convince you that ciphers of this nature are readily soluble, and to give you some insight into the rationale of their development. But be assured that the specimen before us appertains to the very simplest species of cryptograph. It now only remains to give you the full translation of the characters upon the parchment, as unriddled. Here it is :

> ’A good glass in the bishop’s hostel in the devil’s seat forty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death’s-head a bee-line from the tree through the shot fifty feet out.’

Tips for frequency analysis

1. Begin by counting up the frequencies of all the letters in the ciphertext. About five of the letters should have a frequency less than 1 per cent, and these probably represent j, k, q, x and z. One of the letters should have a frequency greater than 10 percent, and it probably represents e.
   The table below shows the average frequencies of all 26 letters in English.



2. If the plaintext doesn’t reveal itself immediately, which is often the case, then focus on pairs of repeated letters. In English the most common repeated letters are ss, ee, tt, ff, ll, mm and oo. If the ciphertext contains any repeated characters, you can assume that they represent one of these.
3. More complex use of statistics can be conceived, such as considering counts of pairs of letters, or triplets (trigrams), and so on. This is done to provide more information to the cryptanalyst, for instance, q and u nearly always occur together in that order in English, even though q itself is rare. Also,*th* is the most common bigram, and *the* the most common trigram.
4. One of the most useful skills for a cryptanalyst is th eability to identify words, or even entire phrases, based on experience or sheer guesswork. Any such word or phrase is known as a *crib*.

Breaking a substitution code	Season	03
	Episode	12
	Document	Cipher 1

```
dsmuayrbmbbmgykmrbluhtydyjbyu26,1791nhalhtlh,
yhgamht,mhttnytldclbyu18,1871nhjmuwayblhy,alhtlh,
yhgamht.sykmrmhyhganrsjmcsyjmcndnmh,psnalrlpsyu,
nhvyhclumhtjydsmhndmayhgnhyyuksllungnhmcytcsyd
lhdypclfmpulgumjjmbaydljpicyu.pmucrlfsnrihdljpaycytjy
dsmhnrjrmuylhtnrpamwnhcsyalhtlhrdnyhdyjiryij.nh1991
mpyufydcawfihdcnlhnhgtnffyuyhdyyhgnhykmrdlhrcuid
cytfuljbmbbmgy'rlungnhmapamhr.binacclclayumhdyrm
dsnyvmbaynhcsy19csdyhciuw,csyriddyrrlfcsyfnhnrsytyh
gnhynhtndmcytcsmcbmbbmgy'rjmdsnhykliatsmvykluoyt.
hnhywymuramcyu,csyrdnyhdyjiryijdljpaycytcsypunhcyub
mbbmgysmttyrnghytflucsytnffyuyhdyyhgnhy,mhmrclhnr
snhgawdljpayxtyvndyflucsy19csdyhciuw.bmbbmgynrduy
tncytkncsnhvyhcnhgcsyfnurcjydsmhndmadljpicyucsmcy
vyhcimaawaytcljluydljpayxtyrnghr.
```

Breaking a substitution code

Season	03
Episode	12
Document	Cipher 2

```
flfyjfpsahgypnbaykifhwgbytnyx23,1912fyeeaxetnyx7,
1954.sxifhfyxyklahsjfpsxjfpazafy,lgkazafyfyezbcopgk
bfosxb.pnbaykahgqpxyzgyhaexbxepgwxpsxqfpsxbg
qjgexbyzgjonpxbhzaxyzx.sxobgvaexefyayqlnxypaflq
gbjflahfpagygqpsxzgyzxopgqpsxflkgbapsjfyezgjonpf
pagyiapspsxpnbaykjfzsayx.iapspsxpnbaykpxhp,jxfyi
salx,sxjfexfhakyaqazfypfyezsfbfzpxbahpazfllcobgvgzf
pavxzgypbawnpagypgpsxexwfpxbxkfbeaykfbpaqaza
flaypxllakxyzx:isxpsxbapiallxvxbwxoghhawlxpghfcps
fpfjfzsayxahzgyhzagnhfyezfypsayr.sxlfpxbigbrxefpps
xyfpagyfloschazfllfwgbfpgbc,zbxfpaykgyxgqpsxqab
hpexhakyhqgbfhpgbxe-obgkbfjzgjonpxb,psxfzx,flp
sgnksapifhyxvxbfzpnfllcwnalpayaphqnllqgbj.ay1948
,sxjgvxepgpsxnyavxbhapcgqjfyzsxhpxbpgigbrgyps
xjfyzsxhpxbjfbr1,psxyxjxbkaykfhgyxgqpsxigble'hxf
blaxhppbnxzgjonpxbh.enbaykpsxhxzgyeigbleifbpn
baykigbrxefpwlxpzslxcofbr,psxnr'hzgexwbxfraykzx
ypbx,fyeifhqgbfpajxsxfegqsnp8,psxhxzpagybxhog
yhawlxqgbkxbjfyyfvflzbcopfyflchah.sxexvahxefynj
wxbgqpxzsyamnxhqgbwbxfraykkxbjfyzaosxbh,ayz
lneaykpsxjxpsgegqpsxwgjwx,fyxlxzpbgjxzsfyazfljfz
sayxpsfpzgnleqayehxppaykhqgbpsxxyakjfjfzsayx.
```

Breaking a substitution code	Season Episode Document	03 12 Cipher 3

```
ofeneow."ofen"rexxjwxicctw.,bdwcyjbwhiwu12
,1954,epmfjqwjimdwdyowjmmugddsoweviqu
(ogo),mfjxdpmaesjnuhpjsjxienjcqwuomedcpd
ymaiwjecmfjadwns.fjepinpdk
cdacydwfepadwkecvdeojcqwuomedcowdmdq
dnp,cdmibnurwmoicsrydcj.fjaipbdwcecqixsjc,
cjatjwpju.fepyimfjwaipiqdcqwjmjxezjwmwhqks
wevjw.rexxjwxiccwjqjevjsib.p.sjgwjjecqdxohmjw
pqejcqjywdxyndwesiimnicmeqhcevjwpemuecbd
qiwimdcec1978,icsqhwwjcmnunevjpecmfjpicyw
icqepqdbiuiwji.ec1991,fjawdmjmfjodohniwowjm
mugddsoweviqu(ogo)owdgwix,icsxisjemivienibnj
(mdgjmfjwaemfemppdhwqjqdsj)mfwdhgfohbneq
ymoydwsdacndis,mfjyewpmaesjnuivienibnjowd
gwixexonjxjcmecgohbneq-kjuqwuomdgwiofu.p
fdwmnumfjwjiymjw,embjqixjivienibnjdvjwpjipve
imfjecmjwcjm,mfdhgfrexxjwxiccfippiesfjfiscdoiw
mecempsepmwebhmedcdhmpesjmfjhp.iymjwiw
jodwmywdxwpisimipjqhwemu,ecq.,afdajwjecine
qjcpecgsepohmjaemfwjgiwsmdhpjdymfjwpiingd
wemfxecogo,mfjqhpmdxppjwveqjpmiwmjsiqwe
xecinecvjpmegimedcdyrexxjwxicc,ydwinnjgjsnu
vednimecgmfjiwxpjzodwmqdcmwdniqm.mfjecvj
pmegimedcnipmjsmfwjjujiwp,bhmaipyecinnusw
doojsaemfdhmyenecgqfiwgjp.
```

Breaking a substitution code	Season	03
	Episode	12
	Document	Cipher 4

```
ksdlurugddkgzvny,bskd1947,njwvdvjylrp,dvip
skt,gnljkpoysqklowvk.wvgnywvoksfvnnsksfjsco
myvknjgvdjvlycgy'nrvolkycvdysfvuvjykgjluvdq
gdvvkgdqldrjscomyvknjgvdjv(vvjn)ldrlcvcbvksfc
gy'njscomyvknjgvdjvldrlkygfgjglugdyvuugqvdjv
ulbsklyskp(jnlgu).ksdkgzvnygnsdvsfywvgdzvdy
sknsfywvknlluqskgywc(lusdqigywlrgnwlcgkldru
vdlruvcld).wvgnywvgdzvdysksfywvnpccvykgjtv
pvdjkpoygsdluqskgywcnkj2,kj4,kj5,ldrjs-gdzvdy
sksfkj6.ywv"kj"nyldrnfsk"kgzvnyjgowvk",skluyv
kdlygzvup,"ksd'njsrv".(kj3ilnbkstvdlyknlnvjmkg
yprmkgdqrvzvusocvdy;ngcgulkup,kj1ilndvzvko
mbugnwvr.)wvlunslmywskvrywvcr2,cr4,cr5ldr
cr6jkpoysqklowgjwlnwfmdjygsdn.gd2006,wvo
mbugnwvrwgngdzvdygsdsfywvywkvvbluusyzs
ygdqnpnyvc,ldgddszlygzvzsygdqnpnyvcywlyg
djskosklyvnywvlbgugypfskywvzsyvkysrgnjvkd
ywlyywvgkzsyvilnjsmdyvriwguvnyguuoksyvjyg
dqywvgkzsyvkokgzljp.csnygcoskyldyup,ywgnn
pnyvcrsvndsykvupsdjkpoysqklowplyluu.nylyg
dq"smkrvcsjkljpgnyssgcoskyldy",wvngcmuyldvs
mnupouljvrywkvvbluusygdywvombugjrsclgd.
```

Breaking a substitution code	Season	03
	Episode	12
	Document	Cipher 5

```
baongjdwoyzognh'dwoy'hozzog,bsmktlkg5,1944,
oealefmjpysqmapwgmakhskgszywgposkggmeszp
lbnof-cgjfmjpysqmapwj.wgmgfgovghabafwgns
mszefogkfghgqmggokiaywgiayofezmsiywgiaeeaf
wlegyyeokeyoylygszygfwksnsqjok1965.hozzogak
hiamyokwgnniak'epapgmkgdhomgfyoskeokfmjp
ysqmapwjdaeplbnoewghok1976.oyokymshlfgha
mahofannjkgdigywshszhoeymoblyokqfmjpysqm
apwofcgje,dwofwdgkyzamysdamhesnvokqskgsz
ywgzlkhaigkyanpmsbngieszfmjpysqmapwj,cgjh
oeymoblyosk.oywaebgfsigcksdkaehozzog-wgnn
iakcgjgxfwakqg.ywgamyofnganeseggieyswavg
eyoilnayghywganiseyoiighoaygplbnofhgvgnspig
kyszakgdfnaeeszgkfmjpyoskanqsmoywie,ywga
ejiigymofcgjanqsmoywie.hozzogdaeiakaqgmsz
egflmgejeygiemgegamfwzsmksmywgmkygngf
si,dwgmgwghgeoqkghywgcgjiakaqgigkyamfw
oygfylmgzsmywgphesegflmoyjejeygizsmx.25k
gydsmce.ok1991wgtsokghelkiofmsejeygienab
smaysmoge(okigknspamc,fanozsmkoa)aeahoe
yokqloewghgkqokggm,dsmcokqpmoiamonjskp
lbnofpsnofjaepgfyeszfmjpysqmapwj.aesziaj2007
hozzogmgiaokedoywelk,egmvokqaeoyefwogzeg
flmoyjszzofgm,akhaeavofgpmgeohgky.
```

Breaking a substitution code	Season	03
	Episode	12
	Document	Cipher 6

```
sberadhdirkdndjdyeasljnefjrb5,1523enhhrd
hrn1596.gdyeaepjdnvghrfblzewenhvjqfwlkj
efgdj.wgdirkdndjdvrfgdjraalnezdhhcdwlwgd
vrfgdjsdrnkrnvljjdvwbqewwjrscwdhwlgrzrn
wgd19wgvdnwcjq.irkdndjdyeasljnrnwgdirb
bekdlpaernw-flcjçern.ewekd17gddnwdjdhw
gdhrfblzewrvadjirvd,enhjdzerndhwgdjdplj30
qdeja,jdwrjrnkrn1570.pridqdejarnwlgravejd
djgdyeaadnwwlwgdhrdwlpyljzaeaeidjqtcnrlj
advjdwejq.ewekd24,gddnwdjdhwgdadjirvdl
pwgdhcmdlpndidja.rn1549gdirarwdhjlzdln
ewyl-qdejhrfblzewrvzraarln,enhekernrn1566.
lnslwgwjrfa,gdvezdrnvlnwevwslwgyrwgsllm
alnvjqfwlkjefgqenhvjqfwlblkrawawgdzadbid
a.ygdnirkdndjdjdwrjdhekdh47,gdhlnewdhgr
a1,000brijdaeqdejrnvlzdwlwgdflljrnfejra.gdz
ejjrdhezejrdiejd.rngrajdwrjdzdnw,gdyeaecwg
ljlplidjwydnwqsllmarnvbchrnkwgd‘‘wjervw
dhdavgrppjdalcadvjdwdazenrdjdah’davjrjd’’
(1585).rnwgrasllmgdhdavjrsdhenecwlmdq
vrfgdjgdgehrnidnwdh,rwyeawgdprjawvrfgd
jlpwgrawqfdepwdjsdbbealnlwwlsdwjrirebbq
sjdemesbd.
```

Breaking a substitution code	Season Episode Document	03 12 Cipher 7

```
zfummoxrzozls,hoxa28rkzkjhkx1950,usthx
uvusyjtvykjtvuzutatarzxwnvobxtnykxtvbzy
igyouapkavkrvykgurkfw-cskrkazxwnvuoatf
boxuvyjaogzojjoafwlaogatsxst,thocvvyxkkw
ktxshkmoxkuvgtsuarknkarkavfwrkpkfonkr
hwxupksv,sytjux,tartrfkjtatvjuv.ykytsaovhk
kabkakxtffwxkzobauskrmoxvyustzyukpkjk
avhkztcskyusgoxlgtshwrkmuauvuoazftssu
mukruamoxjtvuoa,tarvykxkmoxkaovxkfkts
krvovyknchfuztvvykvujk.tvbzyi,zozlsgtsvo
frthocvetjksy.kffus’‘‘aoa-skzxkvkazxwnvu
oa"tarvytvaooakytrhkkathfkvomuartgtwv
otzvctffwujnfkjkavvykzoazknv.zozlsgtsuav
xubckr,vyocbyvthocvuvopkxaubyv,tarua
pkavkr,ua1973,gytvytshkzojklaogatsvykx
stkazxwnvuoatfboxuvyj,xktfusuabkffus’ur
kt.bzyitnnktxsaovvoytpkhkkathfkvomuar
tgtwvocskvykurkt,taruatawztsk,vxktvkru
vtszftssumukr,sovytvgykauvgtsxkuapka
krtarnchfusykrhwxupksv,sytjux,tartrfkjta
ua1977,zozls’nxuoxtzyukpkjkavxkjtuakrca
laogacavuf1997.
```

Breaking a substitution code	Season	03
	Episode	12
	Document	Cipher 8

```
eysrtvr,wbiyrcjvennoifrqezjypmjzwjjt801etv
873,weleteoemniypqezb:etrlyeqrknbryilinbj
o,lkrjtzrlz,elzoiyixjo,elzoitiqjo,kilqiyixrlz,kbjqr
lz,yixrkret,qezbjqezrkret,qhlrkret,nbplrkret,
nbplrkrlz,nlpkbiyixrlz,etvqjzjioiyixrlz.eysrtvr
welenritjjortkopnzixoenbp,jlnjkreyypkopnze
teyplrl.bjxecjzbjurolzstiwtojkiovjvjfnyetezri
tiukopnzeteyplrlrteqethlkornzitvjkrnbjortxk
opnzixoenbrkqjllexjl.rtneozrkhyeo,bjrlkojvrz
jvwrzbvjcjyinrtxzbjuojghjtkpeteyplrlqjzbivw
bjojmpceorezritlrtzbjuojghjtkpiuzbjikkhoojt
kjiuyjzzjolkihyvmjeteypdjvetvjfnyirzjvzimoje
skrnbjol(r.j.kopnzeteyplrlmpuojghjtkpetey
plrl).zbrlwelvjzeryjvrtezjfzojkjtzypojvrlkicjoj
vrtzbjizziqeteokbrcjlrtrlzetmhy,eqethlkorn
zitvjkrnbjortxkopnzixoenbrkqjllexjl,wbrkbe
ylikicjolqjzbivliukopnzeteyplrl,jtkrnbjoqjtzl,
kopnzeteyplrliukjozertjtkrnbjoqjtzl,etvlzez
rlzrkeyeteyplrliuyjzzjoletvyjzzjokiqmrtezrit
lrteoemrk.eysrtvreylibevstiwyjvxjiuniypey
nbemjzrkkrnbjolkjtzhorjlmjuiojyjitmezzrlz
eeymjozr.
```

Breaking a substitution code	Season	03
	Episode	12
	Document	Cipher 9

srrszosjlrdx.nfnlq,pnhosjnsrposrdllrdsm,nlrds
mnhosxrnhynirsrznxrwlos,kyoxlnbrdx.ndjdlxd
l,fcrcnlcnmnbnmsojcx,loxldqbyoshosjnsmqd
zbyosm.rcfcnxfnlxcnxfrzm(olcolxcrdjcx)xcnx
znsxczrdjcpgbznosnyysojcx,xcnxomorxowfrz
mxcnx,cnzmnlo’mxzgxrqdsoxmrfs,fnlnyfnglt
dlxnsoswcrzxfrrdxrkpgjznlq-krfyrzkrdyrzvrfrzv
rgny?-nfrzmfcowc,bgnllrwonxors,bzrdjcxosxr
qyngnsoswrsjzdrdlpnllnsmpnjpnrksrdsl,omor
pl,lyrjnslnsmlngosjl,nwrskdlosj,nprzqcrdlrdxq
rdzosjfcowcolrdjcxosvnosxrwrsxzryrzxdzsrkkb
dxfcowcfrdsmnzrdsmpgposmnfcozyfosmrknw
rzm,nfcoqynlcrknwrzm,nwrzmxcnxfrdymlqyo
xnjnosnsmnjnos,frdymhsoxnjnosnsmnjnos,rkf
rzmlfoxcrdxwrppdsownxorsrznsgqrlloboyoxgr
kwrpbosnxors,frzmlfoxcrdxqzrsdswonxors,loj
sokownxorsrzxznslwzoqxorsbdxrdxrkfcowc,sr
xfoxclxnsmosj,fnlbzrdjcxkrzxcnkydi,nwrsxosd
rdl,wrpqnwxnsmydwomkyrf:nsosxdoxors,nvn
woyynxosjkzollrsrkoyydposnxorsnlokwndjcxos
nkynlcrkyojcxsosjrzosnpolxnbzdqxygzolosjxrds
lczrdmnsrbvordllojs-bdxnlojs,nynl,xcnxfrdymyn
lxnsoslxnsxrsygxrvnsolckrzjrrm.

Document 1 Plain texts

Cipher 1

Charles Babbage was born December 26, 1791 in London, England, and died October 18, 1871 in Marylebone, London, England. He was an English mathematician, philosopher, inventor and mechanical engineer who originated the concept of a programmable computer. Parts of his uncompleted mechanisms are on display in the London Science Museum. In 1991 a perfectly functioning difference engine was constructed from Babbage's original plans. Built to tolerances achievable in the 19th century, the success of the finished engine indicated that Babbage's machine would have worked. Nine years later, the Science Museum completed the printer Babbage had designed for the difference engine, an astonishingly complex device for the 19th century. Babbage is credited with inventing the first mechanical computer that eventually led to more complex designs.

Cipher 2

Alan Mathison Turing was born June 23, 1912 and died June 7, 1954. He was an English mathematician, logician and cryptographer. Turing is often considered to be the father of modern computer science. He provided an influential formalisation of the concept of the algorithm and computation with the Turing machine. With the Turing test, meanwhile, he made a significant and characteristically provocative contribution to the debate regarding artificial intelligence : whether it will ever be possible to say that a machine is conscious and can think. He later worked at the National Physical Laboratory, creating one of the first designs for a stored-program computer, the ACE, although it was never actually built in its full form. In 1948, he moved to the University of Manchester to work on the Manchester Mark 1, then emerging as one of the world's earliest true computers. During the Second World War Turing worked at Bletchley Park, the UK's codebreaking centre, and was for a time head of Hut 8, the section responsible for German naval cryptanalysis. He devised a number of techniques for breaking German ciphers, including the method of the bombe, an electromechanical machine that could find settings for the Enigma machine.

Cipher 3

Philip R. "Phil" Zimmermann Jr., born February 12, 1954, is the creator of Pretty Good Privacy (PGP), the most widely used email encryption software in the world. He is also known for his work in VoIP encryption protocols, notably ZRTP and Zfone. He was born in Camden, New Jersey. His father was a concrete mixer truck driver. Zimmermann received a B.S. degree in computer science from Florida Atlantic University in Boca Raton in 1978, and currently lives in the San Francisco Bay Area. In 1991, he wrote the popular Pretty Good Privacy (PGP) program, and made it available (together with its source code) through public FTP for download, the first widely available program implementing public-key cryptography. Shortly thereafter, it became available overseas via the Internet, though Zimmermann has said he had no part in its distribution outside the US. After a report from RSA Data Security, Inc., who were in a licensing dispute with regard to use of the RSA algorithm in PGP, the Customs Service started a criminal investigation of Zimmermann, for allegedly violating the Arms Export Control Act. The investigation lasted three years, but was finally dropped without filing charges.

Cipher 4

Ronald Linn Rivest, born 1947, Schenectady, New York, is a cryptographer. He is the Professor of Computer Science at MIT's Department of Electrical Engineering and Computer Science (EECS) and a member of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL). Ron Rivest is one of the inventors of the RSA algorithm (along with Adi Shamir and Len Adleman). He is the inventor of the symmetric key encryption algorithms RC2, RC4, RC5, and co-inventor of RC6. The "RC" stands for "Rivest Cipher", or alternatively, "Ron's Code". (RC3 was broken at RSA Security during development; similarly, RC1 was never published.) He also authored the MD2, MD4, MD5 and MD6 cryptographic hash functions. In 2006, he published his invention of the ThreeBallot voting system, an innovative voting system that incorporates the ability for the voter to discern that their vote was counted while still protecting their voter privacy. Most importantly, this system does not rely on cryptography at all. Stating "Our democracy is too important", he simultaneously placed ThreeBallot in the public domain.

Cipher 5

Bailey Whitfield 'Whit' Diffie, born June 5, 1944, is a US cryptographer and one of the pioneers of public-key cryptography. He received a Bachelor of Science degree in mathematics from the Massachusetts Institute of Technology in 1965. Diffie and Martin Hellman's paper New Directions in Cryptography was published in 1976. It introduced a radically new method of distributing cryptographic keys, which went far toward solving one of the fundamental problems of cryptography, key distribution. It has become known as Diffie-Hellman key exchange. The article also seems to have stimulated the almost immediate public development of a new class of encryption algorithms, the asymmetric key algorithms. Diffie was Manager of Secure Systems Research for Northern Telecom, where he designed the key management architecture for the PDSO security system for X.25 networks. In 1991 he joined Sun Microsystems Laboratories (in Menlo Park, California) as a Distinguished Engineer, working primarily on public policy aspects of cryptography. As of May 2007 Diffie remains with Sun, serving as its Chief Security Officer, and as a Vice President.

Cipher 6

Blaise de Vigenere was born April 5, 1523and died in 1596. He was a French diplomat and cryptographer. The Vigenère cipher is so named due to the cipher being incorrectly attributed to him in the 19th century. Vigenère was born in the village of Saint-Pourçain. At age 17 he entered the diplomatic service, and remained there for 30 years, retiring in 1570. Five years into his career he was sent to the Diet of Worms as a very junior secretary. At age 24, he entered the service of the Duke of Nevers. In 1549 he visited Rome on a two-year diplomatic mission, and again in 1566. On both trips, he came in contact both with books on cryptography and cryptologists themselves. When Vigenere retired aged 47, he donated his 1,000 livres a year income to the poor in Paris. He married a Marie Vare. In his retirement, he was author of over twenty books including the "Traicté des Chiffres ou Secrètes Manières d'Escrire" (1585). In this book he described an autokey cipher he had invented, it was the first cipher of this type after Bellaso not to be trivially breakable.

Cipher 7

Clifford Cocks, born 28 December 1950, is a British mathematician and cryptographer at GCHQ who invented the widely-used encryption algorithm now commonly known as RSA, about three years before it was independently developed by Rivest, Shamir, and Adleman at MIT. He has not been generally recognised for this achievement because his work was by definition classified information, and therefore not released to the public at the time. At GCHQ, Cocks was told about James H. Ellis' “non-secret encryption" and that no one had been able to find a way to actually implement the concept. Cocks was intrigued, thought about it overnight, and invented, in 1973, what has become known as the RSA encryption algorithm, realising Ellis' idea. GCHQ appears not to have been able to find a way to use the idea, and in any case, treated it as classified, so that when it was reinvented and published by Rivest, Shamir, and Adleman in 1977, Cocks' prior achievement remained unknown until 1997.

Cipher 8

Al-Kindi, who lived approximately between 801 and 873, was an Arab polymath : an Islamic philosopher, scientist, astrologer, astronomer, cosmologist, chemist, logician, mathematician, musician, physician, physicist, psychologist, and meteorologist. Al-Kindi was a pioneer in cryptography, especially cryptanalysis. He gave the first known recorded explanation of cryptanalysis in A Manuscript on Deciphering Cryptographic Messages. In particular, he is credited with developing the frequency analysis method whereby variations in the frequency of the occurrence of letters could be analyzed and exploited to break ciphers (i.e. cryptanalysis by frequency analysis). This was detailed in a text recently rediscovered in the Ottoman archives in Istanbul, A Manuscript on Deciphering Cryptographic Messages, which also covers methods of cryptanalysis, encipherments, cryptanalysis of certain encipherments, and statistical analysis of letters and letter combinations in Arabic. Al-Kindi also had knowledge of polyalphabetic ciphers centuries before Leon Battista Alberti.

Cipher 9

Noon rings out. A wasp, making an ominous sound, a sound akin to a klaxon or a tocsin, flits about. Augustus, who has had a bad night, sits up blinking and purblind. Oh what was that word (is his thought) that ran through my brain all night, that idiotic word that, hard as I'd try to pun it down, was always just an inch or two out of my grasp - fowl or foul or Vow or Voyal ? - a word which, by association, brought into play an incongruous mass and magma of nouns, idioms, slogans and sayings, a confusing, amorphous outpouring which I sought in vain to control or turn off but which wound around my mind a whirlwind of a cord, a whiplash of a cord, a cord that would split again and again, would knit again and again, of words without communication or any possibility of combination, words without pronunciation, signification or transcription but out of which, notwithstanding, was brought forth a flux, a continuous, compact and lucid flow : an intuition, a vacillating frisson of illumination as if caught in a flash of lightning or in a mist abruptly rising to unshroud an obvious sign - but a sign, alas, that would last an instant only to vanish for good.