TRADITIONAL CRYPTOGRAPHY

BREAKING THE CODE

Julian Thijssen & Olaf van Waart

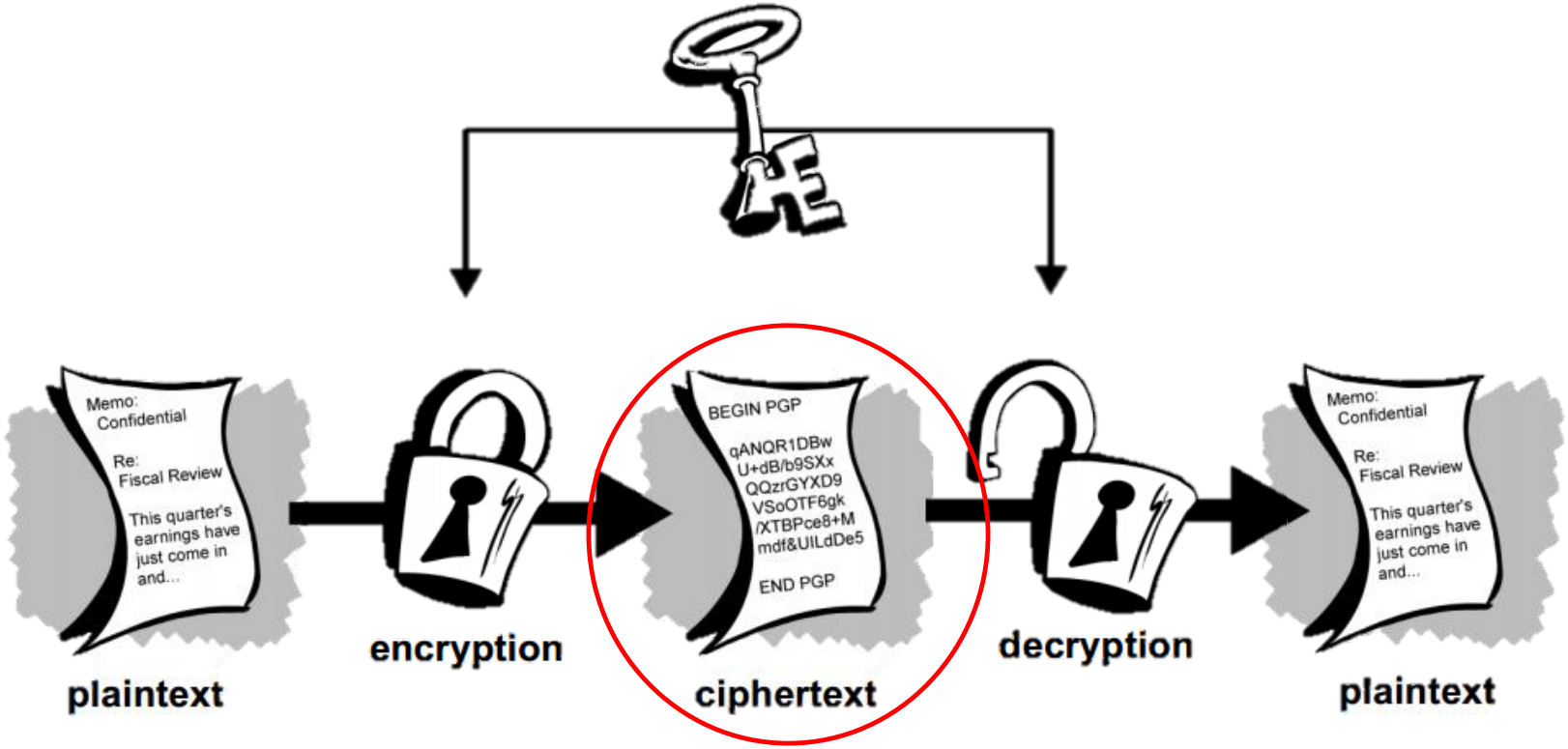
BREAKING THE CODE

1. Introduction to Ciphers
2. Substitution Cipher
3. Permutation Cipher
4. Substitution & Permutation Cipher
5. Polyalphabetic Cipher
6. Periodic Polyalphabetic Cipher
7. Running-Key Ciph
8. Conclusion

BREAKING THE CODE

1. Introduction to Ciphers
2. Substitution Cipher
3. Permutation Cipher
4. Substitution & Permutation Cipher
5. Polyalphabetic Cipher
6. Periodic Polyalphabetic Cipher
7. Running-Key Cipher
8. Conclusion

SYMMETRIC CIPHER



SYMMETRIC CIPHER

Formalized

Given a plaintext P, a key K and ciphertext C.

Encryption:

$$E(K,P) = C$$

Decryption

$$D(K,C) = P$$

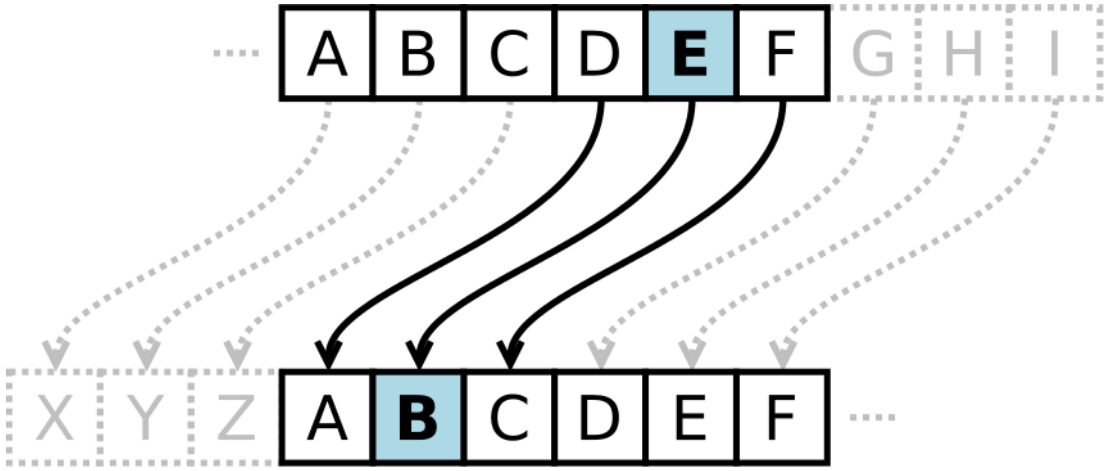
Thus reversible:

$$D(K, E(K,P)) = P$$

CAESAR'S CIPHER

Shifts alphabet by K letters and substitutes each letter in P by it's shifted counterpart.

Example of a left shift 3 Ceasar's cipher (K = −3):



Wikimedia commons - http://en.wikipedia.org/wiki/File:Caesar3.png

CAESAR'S CIPHER

Shifts alphabet by K letters and substitutes each letter in P by it's shifted counterpart.

Each letter is charactarized by it's place in the alphabet thus:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

For $c_i \in C$ and $p_i \in P$

$$c_i = (p_i + K) \; mod \; 26$$

and

$$p_i = (c_i - K) \; mod \; 26$$

EXAMPLE – ENCODE!

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$K = -5$

Plaintext	V	E	N	I
Ciphertext	..	..	..	..

EXAMPLE – ENCODE!

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$K = -5$

Plaintext	V	E	N	I
Ciphertext	Q	Z	I	D

EXAMPLE – DECODE!

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

K = 3

Ciphertext	Y	L	G	L
Plaintext	..	..	..	..

EXAMPLE – DECODE!

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

K = 3

Ciphertext	Y	L	G	L
Plaintext	V	I	D	I

EXAMPLE – BREAK?

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

K = ?

Ciphertext	B	O	I	O
Plaintext	..	..	..	..

EXAMPLE – BREAK?

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

K = ?

Ciphertext	B	O	I	O
Plaintext	V	I	C	I

BREAKING THE CODE

1. Introduction to Ciphers
2. Substitution Cipher
3. Permutation Cipher
4. Substitution & Permutation Cipher
5. Polyalphabetic Cipher
6. Periodic Polyalphabetic Cipher
7. Running-Key Cipher
8. Conclusion

SUBSTITUTION CIPHER

The encoding function substitutes each character of a plaintext, P, according to the substitution alphabet, a.k.a. the key, K.

Example – Alphabet Shuffled:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	T	J	M	V	G	L	N	U	S	R	K	Y	H	A	E	D	P	W	B	C	F	I	O	X	Q

Plaintext: ZIGZAG
Ciphertext: QULQZL

SUBSTITUTION CIPHER

The encoding function substitutes each character of a plaintext, P, according to the substitution alphabet, a.k.a. the key, K.

Example – Alphabet based on other characters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
!	,	\	(	{	?	$	;	*	[	<	|	'	~	\	-	"	^	>	_	@	.	}	%	&	+

Plaintext: ZIGZAG
Ciphertext: +*$+!$

MATHIAS' SUBSTITUTION CIPHER

```
RVRZF19;:-P:8OP-8RHP8:PL1P19RP-LYY8 DP19RZRP;HPLPZL;YOLFPH RRWP;:P19RPH1;ZZ;:-
P8EP19RPS;:WCP:81PYRHHP19L:P;:P19RPS8VRSR:1P8EP19RP78W;RHP8EPSR:DP19RPH8N;LYPL:WP 8Y;1;NLYP
LHH;8:HP9LVRPLNMI;ZRWPHIN9P;:1R:H;1FCPL:WP7RR:PH8PO;WRYFPW;EEIHRWCP19L1P19R;ZP;:RV;1L7YRPZRHIY1HPLZRPLYS8H1P;SSRW;L1RYFP Z8WINRWDP19RP
RZ;8WP8EPHRRWA1;SRPL:WP9LZVRH1P9LHP7RN8SRPLHPH98Z1P;:P 8Y;1;NLYPLHP;1P;HP;:PL-Z;NIY1IZLYPYL78IZDPLPH;:-YRPFRLZP7Z;:-HP;1HPL  Z8
Z;L1RPEZI;1HP18PSL1IZ;1FP;:P19RPS8ZLYPLHP;:P19RP 9FH;NLYPO8ZYWDPR;-91FPFRLZHPRYL HRWP;:PZ8SRPEZ8SP19RP1;SRPO9R:P19RP 8Y;1;NLYP
LHH;8:HPORZRPE;ZH1PH1;ZZRWP7FP1;7RZ;IHP-
ZLNN9IHCP7RE8ZRP;1HPI:ZIYFPN;1;KR:HPORZRPE;:LYYFPHI7WIRWP7FP19RPLZ1CP8ZPWRN;SL1RWP7FP19RPNZIRY1FP8EP8N1LV;IHDPR:-
YL:WPI:WRZOR:1PH;XPFRLZHP8EPN;V;YPOLZPL:WPHIEERZ;:-CP7RE8ZRP19RPLS7;1;8:PL:WPSLW:RHHP8EP19RPY8:-P LZY;LSR:1PORZRPRX RYYRWP7FP19RP IZ-RP8EP
Z;WRCP8ZPNZIH9RWP7FP19RPHO8ZWP8EPNZ8SORYYBP1ORYVRPFRLZHPRYL HRWP7R1ORR:P19RPN8:V8NL1;8:P8EP19RPH1L1RHA-
R:RZLYP;:P,U.GCPL:WP19RPRX1;:N1;8:P8EP19RPY;NR:HRP8EP19RPEZR:N9PZRV8YI1;8:P7FP19RPLZSP8EP:L
8YR8:DP7I1CP8:P19;HP8NNLH;8:CP;:P8:RPFRLZCPLYYCP;:P19RPSRL:1;SRPL1PYRLH1CP9LHP7RR:PLNN8S Y;H9RWDPRZRP19RPYRLVRHCPO9;N9PI:E8YWRWP;:PH Z;:-
PLS;WH1P19RP8VRZ19Z8OP8EP19Z8:RHCPL:WP19RP1ZL:H 8Z1HP8EPZRV8YI1;8:;H1HP8VRZP19RPO8ZYWCP9LWPELYYR:P;:PLI1IS:CP19RP
LHH;8:HPO9;N9P9LWPN8:VIYHRWPSL:T;:WPORZRPNZIH9RWPE8ZP19RP1;SRCPL:WP19RP1Z;IS 9HP8EPWRS8NZLNFPORZRPLZZRH1RWDPLP1RZZ;7YRPZRLN1;8:P9LWPHR1P;:QPRX
RZ;R:NRP8EPHIEERZ;:-P9LWPW8:RP;1HPO8ZTQPL:WPHO;E1PLHP19RPH9LWRHP8EP:;-91P7RE8ZRP19RPZLFHP8EP19RPLHNR:W;:-PHI:CP9LWPW;HL
RLZRWP19RPERZSR:1P8EPZRV8YI1;8:P7RE8ZRP19RPLZ8IHRWP;:W;-:L1;8:P8EP19RPI:N8ZZI 1RWP LZ1P8EPSL:T;:WDP19RPHLSRP LHH;8:HPSLFPL-
L;:PLZ;HRQP19RPHLSRPWRYIH;8:HPL-L;:PH ZRLWCPLHPH;:PH Z;:-HPI PLEZRH9P;:PHINNRHH;VRP-
R:RZL1;8:HP8EPSR:QP7I1PORPT:8OP19RPZRHIY1DP19RFPO;YYCPY;TRP19RPOLFHP8EP19RPI:Z;-91R8IHCP7RPL-L;:PNZIH9RWD
```

BREAKING A SUBSTITUTION CIPHER

Cipher	
Character	Probability
P	0,1686
R	0,1083
1	0,0672
;	0,0630
L	0,0608
H	0,0587
:	0,0576
8	0,0534
Z	0,0534
9	0,0427
W	0,0336
Y	0,0320
E	0,0240
I	0,0240
N	0,0219
S	0,0187
	0,0181
F	0,0144
O	0,0139
-	0,0133
7	0,0133
C	0,0117
V	0,0091
D	0,0064
T	0,0027
Q	0,0021
X	0,0021
A	0,0011
,	0,0005

English	
Character	Probability
	0,1787
e	0,1034
t	0,0692
a	0,0692
i	0,0652
r	0,0602
o	0,0572
s	0,0552
h	0,0532
n	0,0441
d	0,0291
l	0,0271
c	0,0261
p	0,0230
f	0,0200
g	0,0180
w	0,0170
u	0,0160
y	0,0160
b	0,0140
m	0,0110
,	0,0070
v	0,0060
x	0,0040
.	0,0040
k	0,0020
q	0,0010
-	0,0010
j	0,0010

BREAKING A SUBSTITUTION CIPHER

```
eVeZF19;:-_:8O_-8eH_8:_L1_19e_-LYY8 D_19eZe_;H_L_ZL;YOLF_H eeW_;:_19e_H1;ZZ;:-
_8E_19e_S;:WC_:81_YeHH_19L:_;:_19e_S8VeSe:1_8E_19e_78W;eH_8E_Se:D_19e_H8N;LY_L:W_ 8Y;1;NLY_
LHH;8:H_9LVe_LNMI;ZeW_HIN9_;:1e:H;1FC_L:W_7ee:_H8_O;WeYF_W;EEIHeWC_19L1_19e;Z_;:eV;1L7Ye_ZeHIY1H_LZe_LYS8H1_;SSeW;L1eYF_ Z8WINeWD_19e_
eZ;8W_8E_HeeWA1;Se_L:W_9LZVeH1_9LH_7eN8Se_LH_H98Z1_;:_ 8Y;1;NLY_LH_;1_;H_;:_L-Z;NIY1IZLY_YL78IZD_L_H;:-Ye_FeLZ_7Z;:-H_;1H_L  Z8
Z;L1e_EZI;1H_18_SL1IZ;1F_;:_19e_S8ZLY_LH_;:_19e_ 9FH;NLY_O8ZYWD_e;-91F_FeLZH_eYL HeW_;:_Z8Se_EZ8S_19e_1;Se_O9e:_19e_ 8Y;1;NLY_
LHH;8:H_OeZe_E;ZH1_H1;ZZeW_7F_1;7eZ;IH_-
ZLNN9IHC_7eE8Ze_;1H_I:ZIYF_N;1;Ke:H_OeZe_E;:LYYF_HI7WIeW_7F_19e_LZ1C_8Z_WeN;SL1eW_7F_19e_NZIeY1F_8E_8N1LV;IHD_e:-
YL:W_I:WeZOe:1_H;X_FeLZH_8E_N;V;Y_OLZ_L:W_HIEEeZ;:-C_7eE8Ze_19e_LS7;1;8:_L:W_SLW:eHH_8E_19e_Y8:-_ LZY;LSe:1_OeZe_eX eYYeW_7F_19e_ IZ-e_8E_
Z;WeC_8Z_NZIH9eW_7F_19e_HO8ZW_8E_NZ8SOeYYB_1OeYVe_FeLZH_eYL HeW_7e1Oee:_19e_N8:V8NL1;8:_8E_19e_H1L1eHA-
e:eZLY_;:_,U.GC_L:W_19e_eX1;:N1;8:_8E_19e_Y;Ne:He_8E_19e_EZe:N9_ZeV8YI1;8:_7F_19e_LZS_8E_:L
8Ye8:D_7I1C_8:_19;H_8NNLH;8:C_;:_8:e_FeLZC_LYYC_;:_19e_SeL:1;Se_L1_YeLH1C_9LH_7ee:_LNN8S Y;H9eWD_eZe_19e_YeLVeHC_O9;N9_I:E8YWeW_;:_H Z;:-
_LS;WH1_19e_8VeZ19Z8O_8E_19Z8:eHC_L:W_19e_1ZL:H 8Z1H_8E_ZeV8YI1;8:;H1H_8VeZ_19e_O8ZYWC_9LW_ELYYe:_;:_LI1IS:C_19e_
LHH;8:H_O9;N9_9LW_N8:VIYHeW_SL:T;:W_OeZe_NZIH9eW_E8Z_19e_1;SeC_L:W_19e_1Z;IS 9H_8E_WeS8NZLNF_OeZe_LZZeH1eWD_L_1eZZ;7Ye_ZeLN1;8:_9LW_He1_;:Q_eX
eZ;e:Ne_8E_HIEEeZ;:-_9LW_W8:e_;1H_O8ZTQ_L:W_HO;E1_LH_19e_H9LWeH_8E_:;-91_7eE8Ze_19e_ZLFH_8E_19e_LHNe:W;:-_HI:C_9LW_W;HL
eLZeW_19e_EeZSe:1_8E_ZeV8YI1;8:_7eE8Ze_19e_LZ8IHeW_;:W;-:L1;8:_8E_19e_I:N8ZZI 1eW_ LZ1_8E_SL:T;:WD_19e_HLSe_ LHH;8:H_SLF_L-
L;:_LZ;HeQ_19e_HLSe_WeYIH;8:H_L-L;:_H ZeLWC_LH_H;:_H Z;:-H_I _LEZeH9_;:_HINNeHH;Ve_-
e:eZL1;8:H_8E_Se:Q_7I1_Oe_T:8O_19e_ZeHIY1D_19eF_O;YYC_Y;Te_19e_OLFH_8E_19e_I:Z;-91e8IHC_7e_L-L;:_NZIH9eWD
```

BREAKING A SUBSTITUTION CIPHER

`eVeZF19;:-_:8O_-8eH_8:_L1_19e_-LYY8 D_19eZe_;H_L_ZL;YOLF_H eeW_;:_19e_H1;ZZ;:-_`

19e is likely supposed to mean "the" which means `1 = t` and `9 = h`.

`eVeZFth;:-_:8O_-8eH_8:_Lt_the_-LYY8 D_theZe_;H_L_ZL;YOLF_H eeW_;:_the_Ht;ZZ;:-_`

Lt is probably 'at' so L = a but theZe coild be both 'r' and 's'.

Ciphertext	Plaintext
P	_
R	e
I	t
9	h
L	a

We need to go deeper!

BREAKING A SUBSTITUTION CIPHER

The nine most frequent bigrams (combinations of two letters) in English:

th, he, in, er, an, re, nd, on, en

The nine most frequent bigrams in the (partial decoded) Cipher:

th, he, ;:, e:, 8E, eW, Ze, 8:, Z;

The five most frequent trigrams (combinations of three letters) in English:

the, and, ing, her, hat

The five most frequent bigrams in the (partial decoded) Cipher:

the, ;8:, 8:H, a:W, 8:e

Cipher		English	
Character	Probability	Character	Probability
P	0,1686		0,1787
R	0,1083	e	0,1034
1	0,0672	t	0,0692
;	0,0630	a	0,0692
L	0,0608	i	0,0652
H	0,0587	r	0,0602
:	0,0576	o	0,0572
8	0,0534	s	0,0552
Z	0,0534	h	0,0532
9	0,0427	n	0,0441
W	0,0336	d	0,0291
Y	0,0320	l	0,0271
E	0,0240	c	0,0261
I	0,0240	p	0,0230
N	0,0219	f	0,0200
S	0,0187	g	0,0180
	0,0181	w	0,0170
F	0,0144	u	0,0160
O	0,0139	y	0,0160
-	0,0133	b	0,0140
7	0,0133	m	0,0110
C	0,0117	,	0,0070
V	0,0091	v	0,0060
D	0,0064	x	0,0040
T	0,0027	.	0,0040
Q	0,0021	k	0,0020
X	0,0021	q	0,0010
A	0,0011	-	0,0010
,	0,0005	j	0,0010

BREAKING A SUBSTITUTION CIPHER

everything now goes on at the gallopD there is a railway speed in the stirring of the mindC not less than in the movement of the bodies of menD the social and political passions have acquired such intensityC and been so widely diffusedC that their inevitable results are almost immediately producedD the period of seedAtime and harvest has become as short in political as it is in agricultural labourD a single year brings its appropriate fruits to maturity in the moral as in the physical worldD eighty years elapsed in rome from the time when the political passions were first stirred by tiberius gracchusC before its unruly citizens were finally subdued by the artC or decimated by the cruelty of octaviusD england underwent six years of civil war and sufferingC before the ambition and madness of the long parliament were expelled by the purge of prideC or crushed by the sword of cromwellB twelve years elapsed between the convocation of the statesAgeneral in ,U.GC

DECIPHERED SUBSTITUTION CIPHER

From: BLACKWOOD'S Edinburgh MAGAZINE. VOL. LXV.

Everything now goes on at the gallop. There is a railway speed in the stirring of the mind, not less than in the movement of the bodies of men. The social and political passions have acquired such intensity, and been so widely diffused, that their inevitable results are almost immediately produced. The period of seed-time and harvest has become as short in political as it is in agricultural labour. A single year brings its appropriate fruits to maturity in the moral as in the physical world. Eighty years elapsed in Rome from the time when the political passions were first stirred by Tiberius Gracchus, before its unruly citizens were finally subdued by the art, or decimated by the cruelty of Octavius. England underwent six years of civil war and suffering, before the ambition and madness of the Long Parliament were expelled by the purge of Pride, or crushed by the sword of Cromwell: twelve years elapsed between the convocation of the States-general in 1789, and the extinction of the license of the French Revolution by the arm of Napoleon. But, on this occasion, in one year, all, in the meantime at least, has been accomplished. Ere the leaves, which unfolded in spring amidst the overthrow of thrones, and the transports of revolutionists over the world, had fallen in autumn, the passions which had convulsed mankind were crushed for the time, and the triumphs of democracy were arrested. A terrible reaction had set in; experience of suffering had done its work; and swift as the shades of night before the rays of the ascending sun, had disappeared the ferment of revolution before the aroused indignation of the uncorrupted part of mankind. The same passions may again arise; the same delusions again spread, as sin springs up afresh in successive generations of men; but we know the result. They will, like the ways of the unrighteous, be again crushed.

WEAKNESS OF A SUBSTITUTION CIPHER

- All frequency properties of the underlying language remain intact.

- Thus are breakable by statistical frequency analysis.

BREAKING THE CODE

1. Introduction to Ciphers
2. Substitution Cipher
3. Permutation Cipher
4. Substitution & Permutation Cipher
5. Polyalphabetic Cipher
6. Periodic Polyalphabetic Cipher
7. Running-Key Cipher
8. Conclusion

PERMUTATION CIPHER

Changes the order of plaintext in blocks of size b.

Example

`Plaintext: HELLO_WORLD_`

`Blocksize: 3`

1	2	3
H	E	L
L	O	_
W	O	R
L	D	_

1	3	2
H	L	E
L	_	O
W	R	O
L	_	D

`Key: 132`

`Cipher: HLEL_OWROL_D`

The cipher gets more secure by increasing b because there are more possible permutations

MATHIAS' PERMUTATION CIPHER

INTBUI BRETHMH ESTIFE, RPIEA C ORPRY UNTT, ITASES BA HRTHO EN HLYGOUTERSDUNY, BDOOFN OE M NSEE S ALL OFSTIERPA HATT, GHANCA YF DOE ITY SNAOUT OS QHE TF NTIOSUETND A, E THTHANIS REREFORO HORTWM NNTEO COG FNDIHN TIR ETATSE HHICW, T NOS I BEO TEECTFEFHY TBD SEANME ICHH WN COETHITUTISTEITS ON HAS LFEVIDOPRSTHI D.CNVIO CLN, OTIP IMGON SEDSREHN TOUPOATINE AND N,OERWTIN ASNVEEWER ITTTH I WYVER HEWAMER F OFKORI BRETHIH MSTIV HA,NDM COGINOO CTE IDECINHH TTWIIASSPE C INSONTNT EIDYARTPO IVISI D INSON REEFA TE,AST INSHASCESOPRM TIF OURODPE E THDCEGRANT STND AE SUOUTORYLICO P,ICHH WBR AO FQ A EOV TERRUAEA C OF RY,UNTW NOSHAFEN E BDOWELOLI THN ITOUNCS TBY RYEGOV HE,ENTMRNAD LN AOD TEUDKE SH T BYSIEO WHETHELIB LER PALRATON TYTCON HE NT.EINERIVPDEHF TOD HATCWE ODS RWO EN,MF R PAETHAS HETIECOM VES ASO TO THEUMTOF SE GS.NHICANIGORC SOR OA CHLIAV HAENGMECOBE WHE TE CRY-ARTFAC OFN, INIOOAD ESTGHANCF YF DOE TY.SNAT NAETH ISNIOGLON NONDRE ERID WECHOBLO THRY ABD IS FEMI INGTGHE THRFORD OE RHE WH TS ROEITPBY E, IESTARNIVIRSTTOR FG TMAS HET BEYERHN TEWERTUASE HND AT VEROANEILIMFA BUT S, WAS ITS LETNOOHORTS DLY HUG DEDIIV THE BY OFYCRIE BH"TE TH,LL OLEH WAL, LBIHNOT NDT BUGINIE BH TT" A,LLIE TN OD AN,MEOAT H TEFRE"F ADER-TE CHDANNCOR APNT AA" ER.HOT IALCSO,NGEACHATERL AONS OTICOLIPF EHAV Y,CUS H T TOEOM THE BEOAT EGR CTSEBJDCH IWHTDE IIVINAT HED AN;ONTS IA, E EVS IPHE TR OCY IOLSPPOOF TON IITEEPRRO HT TNSEUONDCE GOF CTERNMEOVEAS NTUNEOORRFIT S,,OWSLOLN A S ARSSAEECEONSCY ,NCEEQUTAT H TNMAI HETFORF EHF TOS YARTPE EPOSP ODO ATD RISTNMIAON IATHYS ALWE BEEAVCSIN N,SHE TE SRESPUP OFNIOB REETH IONLEL5174 INFO ET, WT, CFE INNHETOSIPOP , ANIO NGEACHEGEN INI OPLRAAN, ONIE WH,NDON PIN O, TRWE RRYA CHT CATHNE IGANEEFF TOABY CTEANGH CL POF OH. TYICLLD OE NOF AWIRE UATLTILSS E OPN I.IONTRANTIOC AED RN A IONTACAE MLRU ND;INK INDANF EFETHFS OTORERTIA PAUTUMS TOYLLNPLAPSU ACHET IER HOTROWEPN U FOA, NTIOANDI LAS IAOR FD RNTIEN GHANCE OF POE TY ACLIDATET SDRIOE P AND S,EALT AN,IONTRAE GRS AFAS ATG NIMRODTO HT IN,AYI OPETHANS ONIIPOL NDTOF CYIRUL HETPAR NGHN TIY AMESE ATE ASTEIFFDT IT TNRE . SME

BREAKING A PERMUTATION CIPHER

Method of breaking

Possible blocksizes can be found by:

$$|C| \bmod b_i = 0$$

Then you can shuffle 'columns' for each possible b_i and find the b_i which gives the highest frequency of common ngrams (like "th")

BREAKING A PERMUTATION CIPHER

Length of Cipher: 2128

Possible blocksizes: [1, 2, 4, 7, 8, 14, 16, 19, 28, 38, 56, 76, 112, 133, 152, 266, 304, 532, 1064]

“TH”-Frequency for first 5 possible blocksizes: {1: 24, 2: 24, 4: 24, 7: 59, 8: 27}

Blocksize = 7

Key = 5641230

MATHIAS' PERMUTATION CIPHER

BUT IN THE BRITISH EMPIRE, FOR A CENTURY PAST, IT HAS BEEN THOROUGHLY UNDERSTOOD, BY MEN OF SENSE OF ALL PARTIES, THAT A CHANGE OF DYNASTY IS OUT OF THE QUESTION, AND THAT THERE IS NO REFORM WORTH CONTENDING FOR IN THE STATE, WHICH IS NOT TO BE EFFECTED BY THE MEANS WHICH THE CONSTITUTION ITSELF HAS PROVIDED. THIS CONVICTION, LONG IMPRESSED UPON THE NATION, AND INTERWOVEN AS IT WERE WITH THE VERY FRAMEWORK OF THE BRITISH MIND, HAVING COME TO COINCIDE WITH THE PASSIONS INCIDENT TO PARTY DIVISIONS IN A FREE STATE, HAS IN PROCESS OF TIME PRODUCED THE STRANGE AND TORTUOUS POLICY WHICH, FOR ABOVE A QUARTER OF A CENTURY, HAS NOW BEEN FOLLOWED IN THIS COUNTRY BY THE GOVERNMENT, AND LAUDED TO THE SKIES BY THE WHOLE LIBERAL PARTY ON THE CONTINENT. DEPRIVED OF THE WATCHWORDS OF MEN, THE PARTIES HAVE COME TO ASSUME THOSE OF THINGS. ORGANIC OR SOCIAL CHANGE HAVE BECOME THE WAR-CRY OF FACTION, INSTEAD OF CHANGE OF DYNASTY. THE NATION IS NO LONGER DRENCHED WITH BLOOD BY ARMIES FIGHTING FOR THE RED OR THE WHITE ROSE, BY PARTIES STRIVING FOR THE MASTERY BETWEEN THE STUART AND HANOVER FAMILIES, BUT IT WAS NOT LESS THOROUGHLY DIVIDED BY THE CRY OF "THE BILL, THE WHOLE BILL, AND NOTHING BUT THE BILL," AT ONE TIME, AND THAT OF "FREE-TRADE AND CHEAP CORN" AT ANOTHER. SOCIAL CHANGE, ALTERATIONS OF POLICY, HAVE THUS COME TO BE THE GREAT OBJECTS WHICH DIVIDE THE NATION; AND, AS IT IS EVER THE POLICY OF OPPOSITION TO REPRESENT THE CONDUCT OF GOVERNMENT AS ERRONEOUS, IT FOLLOWS, AS A NECESSARY CONSEQUENCE, THAT THE MAIN EFFORTS OF THE PARTY OPPOSED TO ADMINISTRATION ALWAYS HAVE BEEN, SINCE THE SUPPRESSION OF THE REBELLION IN 1745, TO EFFECT, WHEN IN OPPOSITION, A CHANGE IN GENERAL OPINION, AND, WHEN IN POWER, TO CARRY THAT CHANGE INTO EFFECT BY A CHANGE OF POLICY. THE OLD LAW OF NATURE IS STILL IN OPERATION. ACTION AND REACTION RULE MANKIND; AND IN THE EFFORTS OF PARTIES MUTUALLY TO SUPPLANT EACH OTHER IN POWER, A FOUNDATION IS LAID FOR AN ENTIRE CHANGE OF POLICY AT STATED PERIODS, AND AN ALTERATION, AS GREAT AS FROM NIGHT TO DAY, IN THE OPINIONS AND POLICY OF THE RULING PARTY IN THE SAME STATE AT DIFFERENT TIMES.

WEAKNESS

With enough computer power each possible ‘anagram’ can theoretically be calculated and thus the code can be brute forced.

Though in practice with large blocksizes this is pretty hard, but then one can probably solve anagrams within the blocksize which also reveals the key and blocksize.

BREAKING THE CODE

1. Introduction to Ciphers
2. Substitution Cipher
3. Permutation Cipher
4. Substitution & Permutation Cipher
5. Polyalphabetic Cipher
6. Periodic Polyalphabetic Cipher
7. Running-Key Cipher
8. Conclusion

MATHIAS' SUBSTITUTION AND PERMUTATION CIPHER

```
QUJTZJQG?DIZJUOUZQ?QZS'?.ZJ'-!FI!TJF?"J-QUJTJIUF!.JE?Q"DJU"FO'ZTZU?ZDJJL?FU.JO-FIT!Z!!IISJ-FM'AIT-
ZJ?Z!QJJ"'IZ.J'..TZIJ!TS'QJJWUX'TZIJF?IFAJAUIZJI!ILJJMTIFFULB?SQI?JU?FZ!ZJT"IZJTZ?DJI-ILJ'I!ZJ'IFQUJTJTZI?.JQZ;!?APJ'FIGJI-
!MUO"?JTJ.FI'S"IJQQZ?JTZDJ?ZUITJJQJ'TTDQJZ"?FIJX'JIATZ-IJF'JZ'O'SQ'J.Q;JZZERJ'KJ"DF?JFZITJ-!IT!OFZIJMT"I?DQJI!O!QJ"FIO'-KJJ"JXZX?KJ'ITJMDQ-
DJI'TOJVI!U?"!KJL?FUZJ?"FUZFFOUTAJLZUTDJQUJTJXX?UBJWT-
F'JDQU!.UJFQ"JFIJ'D'ZJI?!IFUQ?LUTAJZF?"JE!.'JMTQ?JA?JFIAL?UJ"UZ'?Z.'JJF"FMUAJIXTJIP"''Q'ZAJI!ZDJ"IXTSUJZW-
JQUUJQ'QVAIXJKU"JI'ZU!KSQTZIJIISFQJTDUJIFJ'TS'Z'JDXV?JPUJFISITJZJ'T'SQ'!'YXTJIWAM-J!FQ'ITDFU"AJQ?JDJUXII!J".IBJAZ'!"JIITQIQ!VJF''UQ?USS"IJF'ZJT-
K"JUQU?!SLQXOJ.I!?LTSDJ?MI?S!JQIQ"QI"FJ?JLF!'SXO?Z?J"KIZBIIJ-KJ'-!FUJJ-JIQTZ''XTS!AQJW?T!JWJQPU!IQ"QUAUJTJI.S.?F'?UZ-
XMIZ"FJ?J"UJ?QJI.TQJZSXIU."F'JZ'FIUTQJ.FF'UJSFIIS'!A.JITJZJQ!ZU.F?"JM"?JTJIB!IFQIV"JI!"U?J.U'JKJIQZJLAFUJII"?I"FUBHJOWZF??UX"FJ?J,U?XI!IIDJQX'?J'AF?JJZZQL.
JUITJZZQ!IKQJ'JDZ'Z!UJIT!V'V?UZ'?KVO'JFUTQJFF'"SJWZJSO!'LILF?"JIZUZXJFJIIXID!J"I"XJIZTILUIK-J"J"AF'OQ!?I'ZJJIJIZIQ!UJITIUF!.F'SJ"'A!JI?A"JI?TVJIJM?-
VTJ'"FJ"QIVJFZ''?TBJ'UTAJIJQZ?JSJTITJ.UIUTZIJF-
J'!U.TOZOVQ'JXWQJZ!JZUOK?DQJZ!?J.J..IU"ZFJI!TZJUDIIF!LDJTMI'FDJ'XIZ.JXXJ?JJIDTZSZTI!IFQ"I.'JJQJISF'UBSF'J"'IZTZIJ.JM?Z."JI"FZSIIZFUJJ"IQX?KZ?ZJ-
UTFS?TZIJLQUL"JIS.?!SJTXOILJ!??JF'ZFF'UJZFJISJ"VF?QUI?!Z!T'D?X"J-ITJJWJ"Z?TFIJP?JQQUTJZ??ITZIJZZR!IJZU-
AIJ.Z'JQJSITX'Y'TA'M'!"FJ?JJQT?DFUL"UQUJTJISJ?.TJUFU?TFJQJE?Q"ZJT"FTLJO''K-
J?J.D'JI"!F'JXQO.U!ZUVF?"JQ!Z'QJFJILFMIJB!JQF?DKJ?D'"IJTZZJIFUMQJ!?J"QF?UKFK'X?'JLJW""OTJ?W!QUM!!'TJDJJ"K?TJFLIIFULBUAUJTJIB!J?IQBJ-
JIX!IOZ!SIQJZMIJXQXU"'J'Z!IJB'MAJUT!VIAUFULQQ'VFOJAUJTJJIFTZQIQSIJ-'ZUI!ZJ.FUL!UZF'UJQUJTJA'M'!J'QZJJP.IIJAL'!ZJT"'.J'Z?BUIL!QQJIFVJ!FU!IJ-
?J"!F?FIZVIISMF?UTSDJTJIMT''JZJTSJOA!?II.DJ'M"J"FXOKJIZ'Q?UIJ'JK-
XFUI?Z!.'J"UTQJA..I'J"IJ"FJ""F?OLQQUJ"QIZ''XTSXIX.YWQJD'FJ'ITZJTMD.I'!IJM?I!IQM'!"FJ?JI"J?AJQDUTZJ'-
?"!Q?DITJZJ!'M'"JF"UJLFJU'SUTTDJITTJ?JL"?JFZU?FISJ'ZFIO'TZIJ!IRSIJUZ'?!?JFQF'VUJ""IJZFLFIU.'J.Q!ITJZJQ-M'K'TJDJIU"!SQ?JJMVJ?IT"IJQQAIMTZ'LMCJ'TOZJUTIZJJC?
..J'"FD'IXXUTAJ"ZFUOJTZIJX?QDJ-AUJTJIZ!FIITJZJQOI'TITFJWJMT-!BIID'DJ?M!TZIJQXF-
'J"?JXJJ'"TDFJ'"UVOKJZ"UJ?!EAJUTM!J'.O'LTZ!LIJTJITFIKJI"?IB"?TJFQUJU"QJ'S?I!LJX?O.F?FAJZJ'!I"!Q?DAUMTJJISTJ"XJO'JZK'F.JIZO"JUXII!QZQJ"ZIQIQIJ'AUJTJIV?V?X?A
J!JZKQ'IPF'!!?ZITJWT"IZQUJI!JIXXKAIIAM"JI!ZJTFUUA"JI'J.ZQQUJTJM-
J'HZ?JTZJZ?OKDIJ.J!OQ'T"?JTJV?QXIQJU"IJITSFI.XJIX?XJZITJZJZIS!DF"IIT'J.QQIFJ'JVV'OQJ"ZIQIKJJ'XUZOL.'JJ-
.IZTZDCTJWZJTZ?CMJFIQJ?ITZJ'"UAUQTJM.JXIQOZACJIZKJ.JIITFULXI.'JJQJADUTQJZ'TQ"JF?BFU'S"IJZSZJT.'!SUJIJM?IAZJT"F.I'!ITJ?I!'FZJQITJZJQFS'SQOF'UJQ'QIFUFJ.FISS'
'ZJJIVV'OQTJUZ!UJJNAFF'?SU.FJZFUJJ"TJI-AJZZ!?VOKJ'"UJ?!MACUTJIQTJM"JU?TJIQ?''PZJ'I!LJ?JFILIF"J"J-ZKJTJ?IT?JF"FIX"J"ITAZJ!S'?JZJTQQ?XDJIJJJWF
```

FREQUENCIES!

Cipher		English	
Character	Probability	Character	Probability
J	0,1770		0,1787
I	0,1026	e	0,1034
Z	0,0664	t	0,0692
'	0,0650	a	0,0692
T	0,0599	i	0,0652
F	0,0580	r	0,0602
?	0,0562	o	0,0572
U	0,0558	s	0,0552
Q	0,0536	h	0,0532
"	0,0453	n	0,0441
!	0,0438	d	0,0291
,	0,0245	l	0,0271
X	0,0223	c	0,0261

BLOCKSIZES

Length of Ciphertext: 2740

Possible Blocksizes: [1, 2, 4, 5, 10, 20, 137, 274, 548, 685, 1370]

Most frequent letter at beginning of a word is T, at the end of a word both T and E are very common.

The variant with most ‘t ’, ‘ t’ and ‘e ’ has:

Blocksize: 5
Key: 43102

And looks like this:

```
tTUQ D?Q GOUte Q?tUQ.?St'!- t' TeF!- ?F" TUQ .!UeF"QE ?F" DUtT'Ot D?UtUFL ?F- .O!tTe! Se!eA'F-
```

SUBSTITUTION CIPHER

tTUQ D?Q GOUte Q?tUQ.?St'!- t' TeF!- ?F" TUQ .!UeF"QE ?F" DUtT'Ot D?UtUFL ?F- .O!tTe! Se!eA'F-M tTe- Qt?!te" '.. .'! tTe QST''XW UF tTe Ae?F tUAe L!eeFeM T?BUFL ?QSe!t?UFe" tT?t tTe- De!e L'Fe t' TUQ .?tTe!;Q t' A?Pe eFGOU!-M T?" S'F.eQQe" tT?t Ut D?Q Te DT' T?" Qt'XeF tTe A'Fe- 'Ot '. QS'tt;Q K'RE ?F" DTeF tTe- !etO!Fe"M Te D?Q QO!!'OF"e" K- ?XX tTe K'-QM DT' De!e OVK!?U"UFL ?F" t?OFtUFL TUA DUtT TUQ BUXX?F-W TUQ 'DF .!UeF"Q t'' De!e ?L?UFQt TUAE ?F"M .!'A QT?Ae ?F" ?LUt?tU'F '. AUF"M Te X''Pe" A'Qt D!etSTe"X-W Ut UQ UAV'QQUKXe t' "eQS!UKe tTe QSeFe DTUST F'D t''P VX?Se UF tTe QST''XY!''AW TeF!-M DT'Qe AUF" D?Q !eXUeBe" .!'A tTe "eV!eQQU'F 'SS?QU'Fe" K- tTUQ "UQL!?Se.OX ST?!LeM D?Q S?!eQQe" ?F" S'FL!?tOX?te" K- eBe!- K'- UF tTe QST''XW A!QW T?!!UQ PUQQe" TUA ?..eStU'F?teX-M ?F" Q?U" QTe .eXt S'F.U"eFt '. TUQ UFF'SeFSe .!'A tTe .U!QtM ?F" T?" FeBe! "eQV?U!e" '. UtQ KeUFL A?"e eBU"eFtW HOXU?F? ?F" eXU,? De!e ?XQ' ?A'FLQt tTe .U!Qt t' KeQt'D tTeU! ?VV!'K?tU'F OV'F TUQ S'F"OStW Le'!Le ?F" XUttXe Fe" De!e "eXULTte" Ke-'F" Ae?QO!e t' Qee tTeU! .!UeF" 'FSe A'!e A?"e T?VV-M ?F" T'Ve" Q''F t' T?Be TUA ?Q tTe STUe. UF tTeU! -'OtT.OX QV'!tQW KOt Ut D?Q .?! "U..e!eFt DUtT L!eeFeM DT' F'D .eXt ?XX tTe D!etSTe"FeQQ '. 'Fe S'FBUSte" '. tTe.tM ?F" "eteSte" UF K?QeX- ?tt?STUFL tTe "UQL!?Se.OX ST?!Le t' ?F UFF'SeFt ?F" V!?UQeD'!tT- X?"W Te T?" t?PeF TUQ Qe?t ?t tTe eRt!eAUt- '. tTe QST''XY!''AM ?F" D?Q TU"UFL TUQ .?Se UF TUQ T?F"QE ?F" tT'OLT ? K'- '. D'F"e!.OX QVU!UtQ ?F" Qt!'FL Fe!BeM D?Q F'D K?tTe" UF te?!QM ?F" Q'KKUFL ?X'O"W "!W T?!!UQM DT' T?" KeeF LUBUFL TUA ? Be!- QeBe!e XeStO!eM QtUXX Qt''" 'Be! TUAM UAV!eQQUFL OV'F TUA tTe FeSeQQUt- '. !etU!UFL UFt' TUQ !''AM t' QeeP .!'A L'" tT?t .'!LUBeFeQQ UF V!?-e! ?F" !eVeFt?FSeM DTUSTM Te t'' AOST .e?!e"M D'OX" F't Ke e?QUX- 'Kt?UFe" .!'A TUQ '..eF"e" ?F" "UQLOQte" QST''XY.eXX'DQW Te F'DM tTe!e.'!eM ?!'QeM ?F" A?"e TUQ D?- t'D?!"Q tTe "''!M UF "'UFL DTUST Te T?" ?L?UF t' eFS'OFte! tTe eReS!?tU'FQ ?F" V'UFte" .UFLe!Q '. tTe K'-QM DT' S!Ue"M ?Q Te V?QQe" tTeAM CL'M tT'O tTUe. C ?F" .'XX'De" TUA OFtUX tTe- Q?D TUA eFte! tTe T'OQeW TeF!-M T'DeBe!M D?Q tTe 'FX- X?" DT' "U" F't OVK!?U" TUAE .'!M tT'OLT L!eeFe T?" KeT?Be" UF Q' "UQL!?Se.OX ? A?FFe! t'D?!"Q TUAM Te S'OX" F't KOt .eeX "UQt!eQQe" t' Qee TUA ?VVe?! ?XA'Qt K!'PeFTe?!te"W Te QtUXX !eAeAKe!e"M UF tTe AU"Qt '. TUQ H'-M tT?t KOt ? .eD T'O!Q T?" eX?VQe" QUFSe Te .eXt ?XX tTe D!etSTe"FeQQ '. 'Fe QOVV'Qe" t' Ke LOUXt- '. tTe.tW CDT?t tTeFMC Te Q?U" t' TUAQeX.M CAOQt Ke tTe .eeXUFLQ '. TUA DT' Qt?F"Q S'FBUSte" '. tTe S!UAeM ?F" tTe!e.'!e T?Q F't tTe S'FQSU'OQFeQQ '. UFF'SeFSe t' QOVV'!t TUAN U S?FF't .UF" UF A- Te?!t t' OVK!?U" TUAMC Te Q?U"M ?Q Te t''P Le'!Le ?F" Fe" K- tTe T?F" ?F" Xe" tTeA ?S!'QQ tTe X?DFW

NGRAMS

Most common trigrams in the ciphertext:

```
tTe, ?F”, eQQ, DT’, TUA, UFL
```

Most common trigrams in English:

```
the, and, ing, her, hat
```

Most common bigrams in the ciphertext:

```
Te, tT, UF, !e, TU, ?F, F”
```

Most common bigrams in English:

```
th, he, in, er, an, re, nd
```

SOLUTION

this was quite satisfactory to henry and his friends; and without waiting any further ceremony, they started off for the school. in the mean time greene, having ascertained that they were gone to his father’s to make enquiry, had confessed that it was he who had stolen the money out of scott’s box; and when they returned, he was surrounded by all the boys, who were upbraiding and taunting him with his villany. his own friends too were against him; and, from shame and agitation of mind, he looked most wretchedly. it is impossible to describe the scene which now took place in the school-room. henry, whose mind was relieved from the depression occasioned by this disgraceful charge, was caressed and congratulated by every boy in the school. mrs. harris kissed him affectionately, and said she felt confident of his innocence from the first, and had never despaired of its being made evident. juliana and eliza were also amongst the first to bestow their approbation upon his conduct. george and little ned were delighted beyond measure to see their friend once more made happy, and hoped soon to have him as the chief in their youthful sports. but it was far different with greene, who now felt all the wretchedness of one convicted of theft, and detected in basely attaching the disgraceful charge to an innocent and praiseworthy lad. he had taken his seat at the extremity of the school-room, and was hiding his face in his hands; and though a boy of wonderful spirits and strong nerve, was now bathed in tears, and sobbing aloud. dr. harris, who had been giving him a very severe lecture, still stood over him, impressing upon him the necessity of retiring into his room, to seek from god that forgiveness in prayer and repentance, which, he too much feared, would not be easily obtained from his offended and disgusted school-fellows. he now, therefore, arose, and made his way towards the door, in doing which he had again to encounter the execrations and pointed fingers of the boys, who cried, as he passed them, "go, thou thief " and followed him until they saw him enter the house. henry, however, was the only lad who did not upbraid him; for, though greene had behaved in so disgraceful a manner towards him, he could not but feel distressed to see him appear almost brokenhearted. he still remembered, in the midst of his joy, that but a few hours had elapsed since he felt all the wretchedness of one supposed to be guilty of theft. "what then," he said to himself, "must be the feelings of him who stands convicted of the crime, and therefore has not the consciousness of innocence to support him! i cannot find in my heart to upbraid him," he said, as he took george and ned by the hand and led them across the lawn.

BREAKING THE CODE

1. Introduction to Ciphers
2. Substitution Cipher
3. Permutation Cipher
4. Substitution & Permutation Cipher
5. Polyalphabetic Cipher
6. Periodic Polyalphabetic Cipher
7. Running-Key Cipher
8. Conclusion

FIRST POLYALPHABETIC CIPHER

Invented by:

Leon Battista Alberti

Works by:

- Using multiple alphabets to encode plain text
- And switches alphabets after several words

http://en.wikipedia.org/wiki/Alberti_cipher_disk

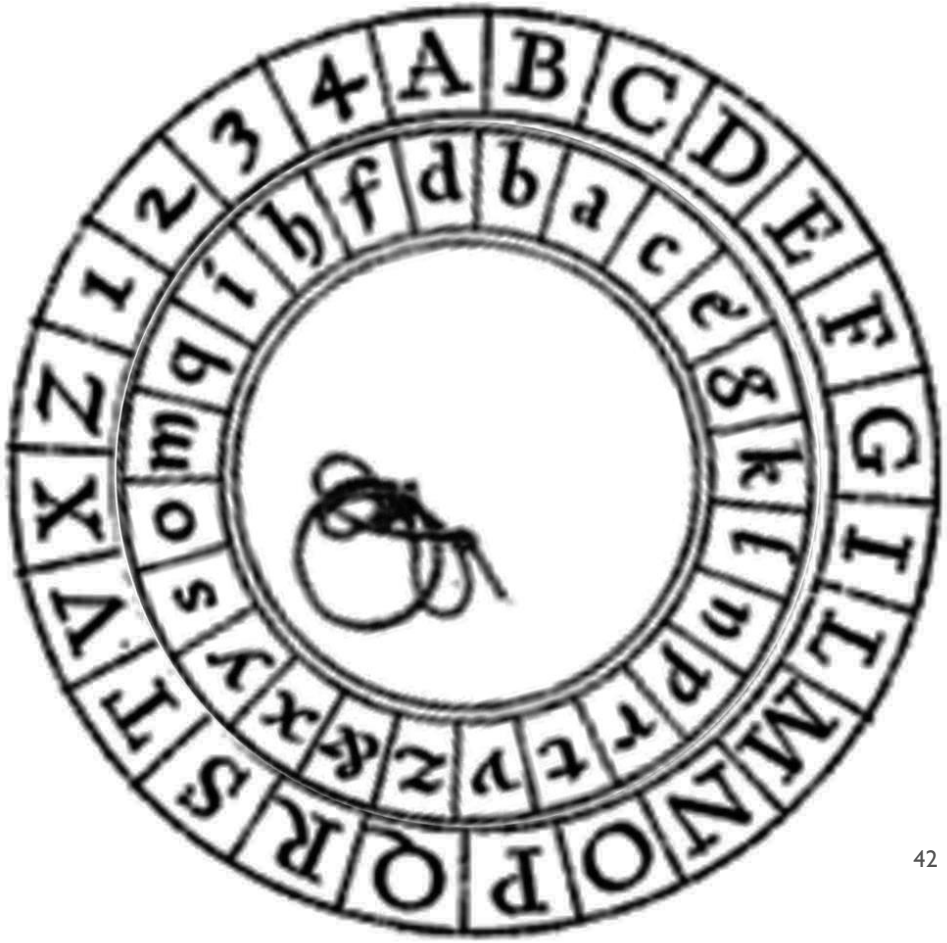
ALBERTI CIPHER

```
plain:  _FLEEAT_ONCE
cipher: ArzppgiFtrae
```

http://en.wikipedia.org/wiki/Alberti_cipher_disk

ALBERTI CIPHER

```
plain:  _FLEEAT_ONCE
cipher: ArzppgiFtrae
```



http://en.wikipedia.org/wiki/Alberti_cipher_disk

TRITHEMIUS CIPHER

Invented by:

Johannes Trithemius

Works by:

- Switching alphabets after every letter
- Uses a tabula recta to determine the next alphabet

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

http://en.wikipedia.org/wiki/Tabula_recta

TRITHEMIUS CIPHER

```
plain:  NEVERMIND
cipher: NFXHVROUL
```

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

http://en.wikipedia.org/wiki/Tabula_recta

VIGENÈRE CIPHER

Invented by:

Giovan Bellaso

Works by:

- Introducing a key to the polyalphabetic cipher
- Switching alphabet every letter according to the key
- Repeating the key along the plaintext

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

http://en.wikipedia.org/wiki/Tabula_recta

EXAMPLE VIGENÈRE

```
plain:  DEFENDTHEWALLS
key:    BLUEBLUEBLUEBL
cipher: EPZIOONLFHUPMD
```

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

http://en.wikipedia.org/wiki/Tabula_recta

PERIODIC POLYALPHABETIC CIPHER

1. Introduction to Ciphers
2. Substitution Cipher
3. Permutation Cipher
4. Substitution & Permutation Cipher
5. Polyalphabetic Cipher
6. Periodic Polyalphabetic Cipher
7. Running-Key Cipher
8. Conclusion

PERIODIC POLYALPHABETIC CIPHER

Properties:

- The frequency distribution is completely flat

How do you recognise it?

- Check for repeating patterns in the ciphertext

- Try some periods and analyse the frequency

PERIODIC POLYALPHABETIC CIPHER

QBRYXGELP;CJ FIOBIBIR.FL-BLFBXUKRLGIEKDTANRWLSKOL'XAJ GVKOLBGBOY'FN'LUUN-PCFX,LLSVJ'QGEKPZR.JAZCGCT'F.CBI AFTIMXIW-
SQFBISKJ,IHL;ZXREZVIZC'XC;EYZZWNK'KFVZLPZGJ,TF.;FIMNEWA,NRD;PECTRFVFIPSVLLEXN-,ERA-LSUGHD'RAKJIXAJAZHE,';;EZVIXBHOI SRLXIELPIHS,V-CAKLZFGFHCUTNLXREG,TF'L' ,JJR-
CVZTZ,HJ,,;;EYPEZS'PIDFJWXCWQNTRNIW-HERYZREL,RFWZNSUREPRF.;NIRXJRZCTJVCDUJ';UE;TIQ.ZF-FWZNSZK;';H.;RIXAJYZ;EKPCSQFBIZEOZ-ZTJB-ZRJ'PFLEPZHS-
PKFBILCUVSPEREZVIZKMLPUAED;PEZVIPAIXXGAJFGCGZAMFTLPIUKRDCUE'W-GAJP;ZWRPRFCF.QUAILLSU'P IECTRFVR,;,AMLLZ;JQ-UKJ,IMXHR UTFLPZGVPKFTL'AP.JY-
F.CBISKUPTRAKL'XNRLRDSOY'.EG,CCBZZIQBRYIONI IZKKLRSVRD;PS;FLU;JYGGX-FIZKKLVCAC.IAXGPCYELPIXNKL;UQFZIUKRPCRN;T-;EZTIR.FLUU.CIPFX,LLSVJWLSA,LGIF;WXZRJ.LZTJV-
UR;TVFX,LEDK,DRUKVPIHXJPTHAI.XZRJ.GFTLPIMXHR ZB',;MAJ'PFU;TRFX,LZGJJZA,A-OISTJAZHELDTFBI.-GT;';FTZLTUTJQ-IX-PIR.C.ISKKDJS;Q, FNIL-BNHR UEZVISKRPVCBR
IZKKLRUQZ.XDKJ.LZTJ.LUETD;PE,,;MBFBIQXQIRFCFLQURELQDGRYHFX,L-OSE,'SXIOIZVJ,;FNKBXRBZTZ,E',PUDQ,C;HJYGQAUPCYELPIMNQF-;E'PECARLTABFFIDFJYXHEZA;FVFI-
MT;';FTZLUUEKDTANRWLU;JD;FTLPIRGCD;FX,LTSGJZXM.CZRLE;TIZ;ZR'SKOL'XB'LEDS-F-F.FLUUR;PJU;JYXOVFIPFTZLUUETP-ABIHIR.FLTSTQ,'SXILQURELXGEL,;;IJ,'FXIW-FDQ,C;BIHIZDCD;HTJ,;.E;T'UG-
XSRBZTIDFJ.LUE,D;ZRJB-,BUPC.EZVIR.FLAGS'XZ,EG,CCNI.MFNIBIAGZKX;BIHIXBHLQSTLL'XAJN-ZK'LGIERPTRBIHI,X-BIHTCT UJ
FI;AU"SXIL'DELDTFWCXTUMJ.LVVNLLZ;JTGRE'DCFG;WLZGKL'ZYFTISTJD;RXJYXHELPZ;ER'IIXEIGQECTIST;T-CN- IUKRDCURMLRSF,PCUKRLPCXHL-
STLPCFTLPIDKFLTVDOPTRAKLU.ELP;CJNLGCERYZRE'PECARIHFT-,;HU;.'U;J.GF.;NI A'DRUERY-FLZZ'MSEIXHEY I,X-BIHTCT UJNLTDUFLTRNRPIAGZQ
UU'LGIEU,TREH,VGBRXCUECTRFBHRGCTCTEUEHDVXTJ.LUKJYZWAJQ-UKJFG,QFBKFN'LXRE'XUHA.X-GTE IRGCTTAB-PRYECI FNE';PECTRFCF.QUAIL'XAJZGZ;'L'XNRLXREG,TF;FVXGBRP
.E'XSAX'PRFTLPI.XQTVFYIDVXTJ,;;ELDTFV.XXCAJAGVRKLWZYFL'XA;ZIABEHCSUCH-YETD;P 'L-OB'FZCBFFIQA-PIMXIF'ZKRIHFUFP'SKOLZG;JZ-MA;KXGDJP;RA-.ZSKHP;REZVIHTCT UJ FI,BFX'UKCT'HHJ,TF'FI
FN'L'XAJ"XA-LQZJJ,UDSROIDCUDGVVE MFKFD'XA-L'XAJ';UE'DRUEI'CFTLPIDTLPCF;CZ-;ER'IXBI.IDFJD'HESXCAX'PIDFJPTABZTZPAJ'CF;FF'SKC.XDKBL;DGJ -
REK,CU;J.GF;;FS,NMLZGJJX;;SFLLZVRPISKJRZCT;TVFTZLSVG'X-FBRFIHAVZ-REG,HLE;.IZR"I AV,WUEIPEUV',C.E,'CFTLPWFTZLG VFZJUEFK-CJJRGHV;Q UESZ-MNQ.XDKJD;FTLPIONR.-CEZVIMXUPCSKOLAAERY-
SGJ.CZBEFMFXIPIIGZNIZKZ.LUGBLZG;NLXGERYXHEG,HYERY-FBITGMAI.IMNQF-FX,L'XB'LCZTLPCFNHXTSKOLVZUFLGIEVZGHVPRACLZF-HEG,TFLFZWSTRPRFTZLVDEQTWDRFF'U;JXSDKJYXHEG,HLERY-
FGZX'UERYZRE'DCFG;WLZGKLLZ;JWLDVFTICAIB-CAKLXREIPEUV',C.E,'CF.;NTUR,LZG;JFFVB-PIRXJ.CUNKLSZTLFIZKKLU.,G,HHEQF-;EVYXUFE I JJR-ZVCT'FFCZWUG'LZG;JFLUASSLUGKPCHMJ,'FT;N-HHJ,PRA-
LZF.F,J.E,, ,EZVICN;TMFVQWLFX,L'XA'PIZVJAGVKKL'XGZXVXERY-FRZAI,J;TVFQCI UJ'LQDSEBI AV'WUEGYG,RMLXOLCFTZCEPMFUCEXGDJD'FKFPRISELPDGJ'ACESD
PG;NTFTZLZQN;.IR.FLRCN;TXGDJ'PFTLPIIRZ'RFBI.GFTLPICBUPCHHJ'CFTZLWZYFL DKOLRUTZXCHER'IMXHPIVLZTIR.FLGR.FZIHBKPKFFZZIR.;FICACFGGHJD'F.CBICACWLU;JA-,RJ, DKOLXGTZLGMTZQ-
CEYPPDGFL'XAMLLZ;JRZHVFBIR.-'AP.J.LUEEDUUGRD-HEZVI A-AXMYJ,;;E'P'FFZ"FSS';FVV"RB'YIHX;IKFBRLQZVJHCD';TVFRC.-FBIL'XAJ,PRA-TGDKJ'PFTLPXCE'PEDKKLRZJJD;FVV",NIBMFNIBIQ.;I-FTLPHF'FZ-
FVTDCRBIHIR.FL-;DFLGIECLCDWTS'ZGIL .BIHISKJH DXH IHAVIAHBZTISKJ.LUEHDR;RFLGIECLRUVZIZRAJNGDGNL'XNRLTSGJZXM.CZRF'CFIOS-B-CXQF .EKPSCBUPRFX,L'XAJF-CQ;W-HEZVIXB'LTNS;Z-FNIBI
GCK-FNR.-G;CT'LERY-CAJYZ;EYP-GEI'IXBI.IDFJ.LUECRSCXCWLFX,L'XAJ.CZDFBHKEI'IMRQPIZVJ.GFTLPIS;FT'STMLGCESXCAX'PIDFJ.LUEV'QZGKIHFLFZSUT-,'DG'LPDRE'QSKOLXRVJ'EMS-Z-
GWFOIOXQT'U;JXSDKJYXHEHP'RRFFGOAJWLZGOPCYEGYXM.NL'XXQHLFSIWGOUZT .ES'QUG,X YEG,TFVZN-
Q.C.IINRDVVAKLUUWCXTUEZVIR.FLWZKMLWSRFFIASRLUU.;TRF.;NIR.C.I;NMJIR.FLHDSIHITK;HLREG,TFG;BXGDJF D'E IZRZTVFVZN-FTG'IXSIBCU;J ZC;'LXGECBJZKVPIDFJQ-
,';HVZGWL'XAJFB.EG,TF.F,J.HJHCZJNLZG;JIGQA-D;PIJ,;;ERY-FCZX ;A-STRGFA;YEH';DTZTGVVE I,AUP FADRZGVFLGIEH'GCECVPDGKD;PEI'IARF,TZKRLZHLFW'FX-LXGTFZ-
HT;TVFWZT'CN'.TFTZL'XAJPHUHJFXCE-DEXN-B.HEO,NUE-PWZBIPRFF;U-;EQRGGERY-FKZBRSKOLLUNKLGIELDTFVR, ,BZTKFVZL;UN-
L'XAJQCSKTLQZVJ.LUEI,CCXGLSZTLLQSKKD;PECIGGDJ.LUEG,'UG'LGIERY-FTCZ;YECTRFVZLAGGQVP,AKLQZVJD'HE'XCINVPMFTL,'FVRP-;ECTRFN-NGCAKLCS;FZIQA-PIOB-ZGCAKLPZBRYPVRE
MFLZD;RE,'CFLZD;RHJQ-GAC.LLELPZCBIHIZE'YZCLJZZRTED;PEZVIHTFP 'VL'RF.Z'PHEYPLSKKLLSUNLZG;JKZPSFIHFUCZJUR;TVFN'L'DERY-FWCXTUEZVIR.;FIVKFUSUWRPRFNIBIVKQFAZRJQACVRLGIEFT-
CDMLAAXIL'XAJRZCTJ'PF.;FIH-QDCUHJ.LUEM'AGDJE;SDL.IRS-T-;HJAXR.J,IHU;I-FSS';F.;FIINVPMFTZLVCAF.I AEAXPDCZ.HECRSCXCWLLER'IXB'LLDG-DPSAKLTVGSZXHAJY-F'CFI

PERIODIC POLYALPHABETIC CIPHER

Method of breaking:

I. Find the greatest common divisor between the distances of the repeating patterns, this is very likely to be the period.

II. Determine the alphabet of the ciphertext, this might give an indication of the plaintext alphabet.

III. Now solve like a substitution cipher for each alphabet using frequency analysis.

PERIODIC POLYALPHABETIC CIPHER

QBRYXGELP;CJ FIOBIBIR.FL-BLFBXUKRLGIEKDTANRWLSKOL'XAJ GVKOLBGBOY'FN'LUUN-PCFX,LLSVJ'QGEKPZR.JAZCGCT'F.CBI AFTIMXIW-
SQFBISKJ,IHL;ZXREZVIZC'XC;EYZZWNK'KFVZLPZGJ,TF.;FIMNEWA,NRD;PECTRFVFIPSVLLEXN-,ERA-LSUGHD'RAKJIXAJAZHE,';;EZVIXBHOI SRLXIELPIHS,V-CAKLZFGFHCUTNLXREG,TF'L' ,JJR-
CVZTZ,HJ,;;EYPEZS'PIDFJWXCWQNTRNIW-HERYZREL,RFWZNSUREPRF.;NIRXJRZCTJVCDUJ';UE;TIQ.ZF-FWZNSZK;';H.;RIXAJYZ;EKPCSQFBIZEOZ-ZTJB-ZRJ'PFLEPZHS-
PKFBILCUVSPEREZVIZKMLPUAED;PEZVIPAIXXGAJFGCGZAMFTLPIUKRDCUE'W-GAJP;ZWRPRFCF.QUAILLSU'P IECTRFVR,;,AMLLZ;JQ-UKJ,IMXHR UTFLPZGVPKFTL'AP.JY-F.CBISKUPTRAKL'XNRLRDSOY'.EG,CCBZZIQBRYIONI
IZKKLRSVRD;PS;FLU;JYGGX-FIZKKLVCAC.IAXGPCYELPIXNKL;UQFZIUKRPCRN;T-;EZTIR.FLUU.CIPFX,LLSVJWLSA,LGIF;WXZRJ.LZTJV-UR;TVFX,LEDK,DRUKVPIHXJPTHAI.XZRJ.GFTLPIMXHR
ZB',;MAJ'PFU;TRFX,LZGJJZA,A-OISTJAZHELDTFBI.-GT;';FTZLTUTJQ-IX-PIR.C.ISKKDJS;Q, FNIL-BNHR UEZVISKRPVCBR IZKKLRUQZ.XDKJ.LZTJ.LUETD;PE,,;MBFBIQXQIRFCFLQURELQDGRYHFX,L-
OSE,'SXIOIZVJ,;FNKBXRBZTZ,E',PUDQ,C;HJYGQAUPCYELPIMNQF-;E'PECARLTABFFIDFJYXHEZA;FVFI-MT;';FTZLUUEKDTANRWLU;JD;FTLPIRGCD;FX,LTSGJZXM.CZRLE;TIZ;ZR'SKOL'XB'LEDS-F-
F.FLUUR;PJU;JYXOVFIPFTZLUUETP-ABIHIR.FLTSTQ,'SXILQURELXGEL,;;IJ,'FXIW-FDQ,C;BIHIZDCD;HTJ,;.E;T'UG-XSRBZTIDFJ.LUE,D;ZRJB-,BUPC.EZVIR.FLAGS'XZ,EG,CCNI.MFNIBIAGZKX;BIHIXBHLQSTLL'XAJN-
ZK'LGIERPTRBIHI,X-BIHTCT UJ FI;AU''SXIL'DELDTFWCXTUMJ.LVVNLLZ;JTGRE'DCFG;WLZGKL'ZYFTISTJD;RXJYXHELPZ;ER'IIXEIGQECTIST;T-CN- IUKRDCURMLRSF,PCUKRLPCXHL-
STLPCFTLPIDKFLTVDOPTRAKLU.ELP;CJNLGCERYZRE'PECARIHFT-,;HU;.'U;J.GF.;NI A'DRUERY-FLZZ'MSEIXHEY I,X-BIHTCT UJNLTDUFLTRNRPIAGZQ UU'LGIEU,TREH,VGBRXCUECTRFBHRGCTCTEUEHDVXTJ.LUKJYZWAJQ-
UKJFG,QFBKFN'LXRE'XUHA.X-GTE IRGCTTAB-PRYECI FNE';PECTRFCF.QUAIL'XAJZGZ;'L'XNRLXREG,TF;FVXGBRP .E'YSAX'PRFTLPI.XQTVFYIDVXTJ,;;ELDTFV.XXCAJAGVRKLWZYFL'XA;ZIABEHCSUCH-YETD;P 'L-
OB'FZCBFFIQA-PIMXIF'ZKRIHFUFP'SKOLZG;JZ-MA;KXGDJP;RA-.ZSKHP;REZVIHTCT UJ FI,BFX'UKCT'HHJ,TF'FI FN'L'XAJ''XA-LQZJJ,UDSROIDCUDGVVE MFKFD'XA-L'XAJ';UE'DRUEI'CFTLPIDTLPCF;CZ-
;ER'IXBI.IDFJD'HESXCAX'PIDFJPTABZTZPAJ'CF;FF'SKC.XDKBL;DGJ -REK,CU;J.GF;;FS,NMLZGJJX;;SFLLZVRPISKJRZCT;TVFTZLSVG'X-FBRFIHAVZ-REG,HLE;.IZR''I AV,WUEIPEUV',C.E,'CFTLPWFTZLG VFZJUEFK-
CJJRGHV;Q UESZ-MNQ.XDKJD;FTLPIONR.-CEZVIMXUPCSKOLAAERY-SGJ.CZBEFMFXIPIIGZNIZKZ.LUGBLZG;NLXGERYXHEG,HYERY-FBITGMAI.IMNQF-FX,L'XB'LCZTLPCFNHXTSKOLVZUFLGIEVZGHVPRACLZF-
HEG,TFLFZWSTRPRFTZLVDEQTWDRFF'U;JXSDKJYXHEG,HLERY-FGZX'UERYZRE'DCFG;WLZGKLLZ;JWLDVFTICAIB-CAKLXREIPEUV',C.E,'CF.;NTUR,LZG;JFFVB-PIRXJ.CUNKLSZTLFIZKKLU.,G,HHEQF-;EVYXUFE I JJR-
ZVCT'FFCZWUG'LZG;JFLUASSLUGKPCHMJ,'FT;N-HHJ,PRA-LZF.F,J.E,, ,EZVICN;TMFVQWLFX,L'XA'PIZVJAGVKKL'XGZXVXERY-FRZAI,J;TVFQCI UJ'LQDSEBI
AV'WUEGYG,RMLXOLCFTZCEPMFUCEXGDJD'FKFPRISELPDGJ'ACESD PG;NTFTZLZQN;.IR.FLRCN;TXGDJ'PFTLPIIRZ'RFBI.GFTLPICBUPCHHJ'CFTZLWZYFL
DKOLRUTZXCHER'IMXHPIVLZTIR.FLGR.FZIHBKPKFFZZIR.;FICACFGGHJD'F.CBICACWLU;JA-,RJ, DKOLXGTZLGMTZQ-CEYPPDGFL'XAMLLZ;JRZHVFBIR.-'AP.J.LUEEDUUGRD-HEZVI A-
AXMYJ,;;E'P'FFZ''FSS';FVV''RB'YIHX;IKFBRLQZVJHCD';TVFRC.-FBIL'XAJ,PRA-TGDKJ'PFTLPXCE'PEDKKLRZJJD;FVV'',NIBMFNIBIQ.;I-FTLPHF'FZ-FVTDCRBIHIR.FL-;DFLGIECLCDWTS'ZGIL .BIHISKJH DXH
IHAVIAHBZTISKJ.LUEHDR;RFLGIECLRUVZIZRAJNGDGNL'XNRLTSGJZXM.CZRF'CFIOS-B-CXQF .EKPSCBUPRFX,L'XAJF-CQ;W-HEZVIXB'LTNS;Z-FNIBI GCK-FNR.-G;CT'LERY-CAJYZ;EYP-
GEI'IXBI.IDFJ.LUECRSCXCWLFX,L'XAJ.CZDFBHKEI'IMRQPIZVJ.GFTLPIS;FT'STMLGCESXCAX'PIDFJ.LUEV'QZGKIHFLFZSUT-,'DG'LPDRE'QSKOLXRVJ'EMS-Z-
GWFOIOXQT'U;JXSDKJYXHEHP'RRFFGOAJWLZGOPCYEGYXM.NL'XXQHLFSIWGOUZT .ES'QUG,X YEG,TFVZN-Q.C.IINRDVVAKLUUWCXTUEZVIR.FLWZKMLWSRFFIASRLUU.;TRF.;NIR.C.I;NMJIR.FLHDSIHITK;HLREG,TFG;BXGDJF D'E
IZRZTVFVZN-FTG'IXSIBCU;J ZC;'LXGECBJZKVPIDFJQ-,';HVZGWL'XAJFB.EG,TF.F,J.HJHCZJNLZG;JIGQA-D;PIJ,;;ERY-FCZX ;A-STRGFA;YEH';DTZTGVVE I,AUP
FADRZGVFLGIEH'GCECVPDGKD;PEI'IARF,TZKRLZHLFW'FX-LXGTFZ-HT;TVFWZT'CN'.TFTZL'XAJPHUHJFXCE-DEXN-B.HEO,NUE-PWZBIPRFF;U-;EQRGGERY-FKZBRSKOLLUNKLGIELDTFVR, ,BZTKFVZL;UN-
L'XAJQCSKTLQZVJ.LUEI,CCXGLSZTLLQSKKD;PECIGGDJ.LUEG,'UG'LGIERY-FTCZ;YECTRFVZLAGGQVP,AKLQZVJD'HE'XCINVPMFTL,'FVRP-;ECTRFN-NGCAKLCS;FZIQA-PIOB-ZGCAKLPZBRYPVRE MFLZD;RE,'CFLZD;RHJQ-
GAC.LLELPZCBIHIZE'YZCLJZZRTED;PEZVIHTFP 'VL'RF.Z'PHEYPLSKKLLSUNLZG;JKZPSFIHFUCZJUR;TVFN'L'DERY-FWCXTUEZVIR.;FIVKFUSUWRPRFNIBIVKQFAZRJQACVRLGIEFT-CDMLAAXIL'XAJRZCTJ'PF.;FIH-
QDCUHJ.LUEM'AGDJE;SDL.IRS-T-;HJAXR.J,IHU;I-FSS';F.;FIINVPMFTZLVCAF.I AEAXPDCZ.HECRSCXCWLLER'IXB'LLDG-DPSAKLTVGSZXHAJY-F'CFI

PERIODIC POLYALPHABETIC CIPHER

Method of breaking:

I. Find the greatest common divisor between the distances of the repeating patterns, this is very likely to be the period.

II. Determine the alphabet of the ciphertext, this might give an indication of the plaintext alphabet.

III. Now solve like a substitution cipher for each alphabet using frequency analysis.

PERIODIC POLYALPHABETIC CIPHER

QBRYXGELP;CJ FIOBIBIR.FL-BLFBXUKRLGIEKDTANRWLSKOL'XAJ GVKOLBGBOY'FN'LUUN-PCFX,LLSVJ'QGEKPZR.JAZCGCT'F.CBI AFTIMXIW-
SQFBISKJ,IHL;ZXREZVIZC'XC;EYZZWNK'KFVZLPZGJ,TF.;FIMNEWA,NRD;PECTRFVFIPSVLLEXN-,ERA-LSUGHD'RAKJIXAJAZHE,';;EZVIXBHOI SRLXIELPIHS,V-CAKLZFGFHCUTNLXREG,TF'L' ,JJR-
CVZTZ,HJ,;;EYPEZS'PIDFJWXCWQNTRNIW-HERYZREL,RFWZNSUREPRF.;NIRXJRZCTJVCDUJ';UE;TIQ.ZF-FWZNSZK;';H.;RIXAJYZ;EKPCSQFBIZEOZ-ZTJB-ZRJ'PFLEPZHS-
PKFBILCUVSPEREZVIZKMLPUAED;PEZVIPAIXXGAJFGCGZAMFTLPIUKRDCUE'W-GAJP;ZWRPRFCF.QUAILLSU'P IECTRFVR,;,AMLLZ;JQ-UKJ,IMXHR UTFLPZGVPKFTL'AP.JY-F.CBISKUPTRAKL'XNRLRDSOY'.EG,CCBZZIQBRYIONI
IZKKLRSVRD;PS;FLU;JYGGX-FIZKKLVCAC.IAXGPCYELPIXNKL;UQFZIUKRPCRN;T-;EZTIR.FLUU.CIPFX,LLSVJWLSA,LGIF;WXZRJ.LZTJV-UR;TVFX,LEDK,DRUKVPIHXJPTHAI.XZRJ.GFTLPIMXHR
ZB',;MAJ'PFU;TRFX,LZGJJZA,A-OISTJAZHELDTFBI.-GT;';FTZLTUTJQ-IX-PIR.C.ISKKDJS;Q, FNIL-BNHR UEZVISKRPVCBR IZKKLRUQZ.XDKJ.LZTJ.LUETD;PE,,;MBFBIQXQIRFCFLQURELQDGRYHFX,L-
OSE,'SXIOIZVJ,;FNKBXRBZTZ,E',PUDQ,C;HJYGQAUPCYELPIMNQF-;E'PECARLTABFFIDFJYXHEZA;FVFI-MT;';FTZLUUEKDTANRWLU;JD;FTLPIRGCD;FX,LTSGJZXM.CZRLE;TIZ;ZR'SKOL'XB'LEDS-F-
F.FLUUR;PJU;JYXOVFIPFTZLUUETP-ABIHIR.FLTSTQ,'SXILQURELXGEL,;;IJ,'FXIW-FDQ,C;BIHIZDCD;HTJ,;.E;T'UG-XSRBZTIDFJ.LUE,D;ZRJB-,BUPC.EZVIR.FLAGS'XZ,EG,CCNI.MFNIBIAGZKX;BIHIXBHLQSTLL'XAJN-
ZK'LGIERPTRBIHI,X-BIHTCT UJ FI;AU''SXIL'DELDTFWCXTUMJ.LVVNLLZ;JTGRE'DCFG;WLZGKL'ZYFTISTJD;RXJYXHELPZ;ER'IIXEIGQECTIST;T-CN- IUKRDCURMLRSF,PCUKRLPCXHL-
STLPCFTLPIDKFLTVDOPTRAKLU.ELP;CJNLGCERYZRE'PECARIHFT-,;HU;.'U;J.GF.;NI A'DRUERY-FLZZ'MSEIXHEY I,X-BIHTCT UJNLTDUFLTRNRPIAGZQ UU'LGIEU,TREH,VGBRXCUECTRFBHRGCTCTEUEHDVXTJ.LUKJYZWAJQ-
UKJFG,QFBKFN'LXRE'XUHA.X-GTE IRGCTTAB-PRYECI FNE';PECTRFCF.QUAIL'XAJZGZ;'L'XNRLXREG,TF;FVXGBRP .E'YSAX'PRFTLPI.XQTVFYIDVXTJ,;;ELDTFV.XXCAJAGVRKLWZYFL'XA;ZIABEHCSUCH-YETD;P 'L-
OB'FZCBFFIQA-PIMXIF'ZKRIHFUFP'SKOLZG;JZ-MA;KXGDJP;RA-.ZSKHP;REZVIHTCT UJ FI,BFX'UKCT'HHJ,TF'FI FN'L'XAJ''XA-LQZJJ,UDSROIDCUDGVVE MFKFD'XA-L'XAJ';UE'DRUEI'CFTLPIDTLPCF;CZ-
;ER'IXBI.IDFJD'HESXCAX'PIDFJPTABZTZPAJ'CF;FF'SKC.XDKBL;DGJ -REK,CU;J.GF;;FS,NMLZGJJX;;SFLLZVRPISKJRZCT;TVFTZLSVG'X-FBRFIHAVZ-REG,HLE;.IZR''I AV,WUEIPEUV',C.E,'CFTLPWFTZLG VFZJUEFK-
CJJRGHV;Q UESZ-MNQ.XDKJD;FTLPIONR.-CEZVIMXUPCSKOLAAERY-SGJ.CZBEFMFXIPIIGZNIZKZ.LUGBLZG;NLXGERYXHEG,HYERY-FBITGMAI.IMNQF-FX,L'XB'LCZTLPCFNHXTSKOLVZUFLGIEVZGHVPRACLZF-
HEG,TFLFZWSTRPRFTZLVDEQTWDRFF'U;JXSDKJYXHEG,HLERY-FGZX'UERYZRE'DCFG;WLZGKLLZ;JWLDVFTICAIB-CAKLXREIPEUV',C.E,'CF.;NTUR,LZG;JFFVB-PIRXJ.CUNKLSZTLFIZKKLU.,G,HHEQF-;EVYXUFE I JJR-
ZVCT'FFCZWUG'LZG;JFLUASSLUGKPCHMJ,'FT;N-HHJ,PRA-LZF.F,J.E,, ,EZVICN;TMFVQWLFX,L'XA'PIZVJAGVKKL'XGZXVXERY-FRZAI,J;TVFQCI UJ'LQDSEBI
AV'WUEGYG,RMLXOLCFTZCEPMFUCEXGDJD'FKFPRISELPDGJ'ACESD PG;NTFTZLZQN;.IR.FLRCN;TXGDJ'PFTLPIIRZ'RFBI.GFTLPICBUPCHHJ'CFTZLWZYFL
DKOLRUTZXCHER'IMXHPIVLZTIR.FLGR.FZIHBKPKFFZZIR.;FICACFGGHJD'F.CBICACWLU;JA-,RJ, DKOLXGTZLGMTZQ-CEYPPDGFL'XAMLLZ;JRZHVFBIR.-'AP.J.LUEEDUUGRD-HEZVI A-
AXMYJ,;;E'P'FFZ''FSS';FVV''RB'YIHX;IKFBRLQZVJHCD';TVFRC.-FBIL'XAJ,PRA-TGDKJ'PFTLPXCE'PEDKKLRZJJD;FVV'',NIBMFNIBIQ.;I-FTLPHF'FZ-FVTDCRBIHIR.FL-;DFLGIECLCDWTS'ZGIL .BIHISKJH DXH
IHAVIAHBZTISKJ.LUEHDR;RFLGIECLRUVZIZRAJNGDGNL'XNRLTSGJZXM.CZRF'CFIOS-B-CXQF .EKPSCBUPRFX,L'XAJF-CQ;W-HEZVIXB'LTNS;Z-FNIBI GCK-FNR.-G;CT'LERY-CAJYZ;EYP-
GEI'IXBI.IDFJ.LUECRSCXCWLFX,L'XAJ.CZDFBHKEI'IMRQPIZVJ.GFTLPIS;FT'STMLGCESXCAX'PIDFJ.LUEV'QZGKIHFLFZSUT-,'DG'LPDRE'QSKOLXRVJ'EMS-Z-
GWFOIOXQT'U;JXSDKJYXHEHP'RRFFGOAJWLZGOPCYEGYXM.NL'XXQHLFSIWGOUZT .ES'QUG,X YEG,TFVZN-Q.C.IINRDVVAKLUUWCXTUEZVIR.FLWZKMLWSRFFIASRLUU.;TRF.;NIR.C.I;NMJIR.FLHDSIHITK;HLREG,TFG;BXGDJF D'E
IZRZTVFVZN-FTG'IXSIBCU;J ZC;'LXGECBJZKVPIDFJQ-,';HVZGWL'XAJFB.EG,TF.F,J.HJHCZJNLZG;JIGQA-D;PIJ,;;ERY-FCZX ;A-STRGFA;YEH';DTZTGVVE I,AUP
FADRZGVFLGIEH'GCECVPDGKD;PEI'IARF,TZKRLZHLFW'FX-LXGTFZ-HT;TVFWZT'CN'.TFTZL'XAJPHUHJFXCE-DEXN-B.HEO,NUE-PWZBIPRFF;U-;EQRGGERY-FKZBRSKOLLUNKLGIELDTFVR, ,BZTKFVZL;UN-
L'XAJQCSKTLQZVJ.LUEI,CCXGLSZTLLQSKKD;PECIGGDJ.LUEG,'UG'LGIERY-FTCZ;YECTRFVZLAGGQVP,AKLQZVJD'HE'XCINVPMFTL,'FVRP-;ECTRFN-NGCAKLCS;FZIQA-PIOB-ZGCAKLPZBRYPVRE MFLZD;RE,'CFLZD;RHJQ-
GAC.LLELPZCBIHIZE'YZCLJZZRTED;PEZVIHTFP 'VL'RF.Z'PHEYPLSKKLLSUNLZG;JKZPSFIHFUCZJUR;TVFN'L'DERY-FWCXTUEZVIR.;FIVKFUSUWRPRFNIBIVKQFAZRJQACVRLGIEFT-CDMLAAXIL'XAJRZCTJ'PF.;FIH-
QDCUHJ.LUEM'AGDJE;SDL.IRS-T-;HJAXR.J,IHU;I-FSS';F.;FIINVPMFTZLVCAF.I AEAXPDCZ.HECRSCXCWLLER'IXB'LLDG-DPSAKLTVGSZXHAJY-F'CFI

PERIODIC POLYALPHABETIC CIPHER

Method of breaking:

I. Find the greatest common divisor between the distances of the repeating patterns, this is very likely to be the period.

II. Determine the alphabet of the ciphertext, this might give an indication of the plaintext alphabet.

III. Now solve like a substitution cipher for each alphabet using frequency analysis.

PERIODIC POLYALPHABETIC CIPHER

```
QBRYX    FX,LL    FVZLP
GELP;    SVJ'Q    ZGJ,T
CJ FI    GEKPZ    F.;FI
OBIBI    R.JAZ    MNEWA
R.FL-    CGCT'    ,NRD;
BLFBX    F.CBI    PECTR
UKRLG     AFTI    FVFIP
IEKDT    MXIW-    SVLLE
ANRWL    SQFBI    XN-,E
SKOL'    SKJ,I    RA-LS
XAJ G    HL;ZX    UGHD'
VKOLB    REZVI    RAKJI
GBOY'    ZC'XC    XAJAZ
FN'LU    ;EYZZ    HE,';
UN-PC    WNK'K    ;EZVI
```

Cipher		English	
Letter	Probability	Letter	Probability
F	0.1664	_	0.1787
U	0.1113	E	0.1034
Z	0.0773	T	0.0692
R	0.0703	A	0.0692
C	0.0633	I	0.0652
S	0.0586	R	0.0602
H	0.0574	O	0.0572
D	0.0550	S	0.0552
X	0.0457	H	0.0532
G	0.0445	N	0.0441
;	0.0304	D	0.0291
M	0.0269	L	0.0271
,	0.0257	C	0.0261
I	0.0246	P	0.0230
A	0.0199	F	0.0200
P	0.0199	G	0.0180
V	0.0175	W	0.0170
.	0.0175	U	0.0160
Q	0.0140	Y	0.0160
O	0.0140	B	0.0140
_	0.0117	M	0.0110
Y	0.0105	,	0.0070
L	0.0070	V	0.0060
B	0.0023	X	0.0040
W	0.0023	.	0.0040
N	0.0011	K	0.0020
K	0.0011	Q	0.0010
T	0.0011	-	0.0010
'	0.0011	J	0.0010

PERIODIC POLYALPHABETIC CIPHER

Method of breaking:

If the cipher is applied with a tabula recta, you are almost done.

Find one character (like space) for each alphabet and you have the rest of the characters.

PERIODIC POLYALPHABETIC CIPHER

Method of breaking:

If the alphabet is scrambled then manually try to find small words by replacing the highest frequency letters and then expand from there.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	-	'	;	,	.	_
Z	_	M	;	U	I	P	X	S	-	T	,	O	G	D	A	N	C	H	R	V	W	Q	B	.		'	J	K	Y	L	F
N	C	W	;	A	F	D	.	B		Y	R	U	K	X	L	-	G	V	T	S	Q	'		J		,	_	I	H	M	E
C	Y	V	K	F	,	O	L	;	A	T	E	H	I	Z	S	.	-	'	R	Q	U	G	D	M		P	_	B	N	W	J
,	Q	W	B	P	V	H	Y	D	G	E	I	N	T	'	R		Z	F	.	X	K	A	U	_		S	M		J	O	L
Z	U	E	R	-	P	V	L	X	Y	B	_	W	;	G	S	F	C	T	'	A	J	Q	O	H	N		.		M	K	I

BREAKING THE CODE

1. Introduction to Ciphers
2. Substitution Cipher
3. Permutation Cipher
4. Substitution & Permutation Cipher
5. Polyalphabetic Cipher
6. Periodic Polyalphabetic Cipher
7. Running-Key Cipher
8. Conclusion

RUNNING-KEY CIPHER

What is it?

1. Instead of taking a key and repeating it, you take a text from a book that is as long as the plaintext.
2. You then perform some kind of operation between the plaintext and the key (most often XOR or ASCII addition).

RUNNING-KEY CIPHER

```
plain:  DEFEND THE EAST WALL AGAINST THE INVASION
key:    IT WAS GROWING LATE IN THE AFTERNOON WHEN
cipher: □□f□□□@□□□w□□□□tl□□□□li□g□□□s□f¨□□n□□¤aª□□□□
```

RUNNING-KEY CIPHER

149 164 116 114 149 152 142 100 100 156 148 167 105 162 161 101 111 153 117 144 132 147 127 115 151 158 162 64 155 139 115 165 101 170 151 141 163 116 157 151 143 167 76 111 157 104 153 150 101 116 149 134 116 153 151 150 145 145 115 171
111 147 159 151 109 105 149 152 100 98 149 148 134 110 154 148 150 108 133 99 160 138 162 162 64 148 158 150 105 160 140 109 99 168 145 144 162 76 110 157 111 156 117 159 134 161 116 159 161 152 153 155 111 161 101 139 159 148 145 64 149
150 153 143 112 108 148 114 147 139 114 97 155 165 101 163 166 142 161 140 114 159 153 127 64 138 156 100 97 116 159 134 121 116 159 151 158 138 144 116 154 157 145 64 149 156 144 146 142 146 97 163 151 111 151 110 111 147 111 169 154 147
102 165 155 101 149 110 135 111 158 153 148 111 162 148 162 116 104 148 159 145 101 145 146 147 111 101 138 169 101 152 118 101 158 118 156 157 117 149 146 64 156 137 155 101 98 150 152 147 139 64 162 158 97 151 141 101 119 140 142 134
137 121 104 144 153 64 147 141 149 165 165 138 100 111 165 105 162 139 138 64 166 157 142 110 99 158 148 118 169 148 152 105 166 157 165 108 134 115 103 149 150 101 105 158 111 153 153 97 142 158 103 138 156 64 158 137 147 117 132 147 171
101 145 147 115 163 114 64 157 150 147 111 168 134 149 149 152 162 147 64 133 147 135 114 136 138 148 115 148 146 101 150 155 97 143 138 153 105 152 161 115 164 139 100 116 142 151 111 157 114 153 155 138 114 172 138 162 144 99 141 143
146 115 97 157 138 64 155 134 162 117 148 138 104 141 141 154 101 119 139 153 141 110 97 145 134 167 148 155 152 162 166 97 168 141 137 78 112 166 151 137 105 137 154 108 144 148 99 153 104 142 115 115 165 162 151 152 146 151 118 149 147
110 157 151 102 153 111 112 118 97 160 104 145 105 142 138 97 134 121 111 137 111 162 156 138 110 153 151 145 143 97 158 136 152 148 139 155 147 115 99 137 163 150 99 145 110 129 114 114 152 167 149 161 112 105 143 154 64 143 157 114 168
144 101 97 163 104 173 155 142 99 141 145 97 155 148 164 108 147 102 98 169 111 155 153 164 152 150 138 160 101 114 139 149 161 149 146 129 76 110 150 158 144 138 165 64 148 158 155 134 160 153 172 116 132 143 152 140 155 116 119 156 141
147 76 102 160 144 109 134 134 108 97 104 168 150 132 151 108 138 145 158 101 147 151 151 157 143 154 128 105 161 147 109 153 140 171 101 138 167 101 151 146 148 111 167 162 105 149 145 155 101 147 110 147 110 141 124 152 134 108 139 120
163 143 110 155 157 142 156 154 101 136 125 109 157 150 142 111 157 165 98 143 166 111 156 102 116 150 134 116 151 148 143 163 111 149 156 116 149 160 97 133 148 153 114 145 164 162 91 98 154 110 152 104 142 110 171 142 165 146 144 153 64
161 139 118 159 158 163 118 156 137 138 155 136 137 64 162 158 116 114 145 147 151 152 114 99 148 142 148 114 141 174 116 156 151 147 151 116 173 104 142 153 114 148 146 121 116 150 148 109 153 154 130 154 101 157 161 91 104 157 155 101
161 156 110 97 159 138 116 149 148 158 163 158 146 163 115 116 145 141 114 138 161 112 64 151 141 147 116 149 155 135 153 147 134 108 105 148 111 151 153 138 165 121 105 143 103 153 104 148 102 109 157 151 152 108 105 133 152 97 170 113
108 141 110 133 115 116 145 147 64 151 141 147 116 159 134 116 148 152 105 147 145 118 166 155 167 160 141 125 110 130 165 121 109 150 134 156 105 144 161 76 116 150 138 120 170 101 142 138 153 153 110 168 104 149 97 166 155 152 146 153
141 76 97 116 154 138 102 162 151 153 102 139 148 150 113 153 138 167 105 169 134 166 76 112 166 141 149 97 155 147 137 120 145 152 114 157 141 147 99 152 141 103 168 134 141 108 114 111 166 104 134 115 152 157 157 131 154 141 151 149 103
116 141 147 101 150 140 166 123 99 166 137 153 105 149 97 150 144 149 140 148 168 142 64 157 150 137 105 149 134 162 140 148 122 97 160 104 140 117 142 155 146 115 108 134 151 64 171 156 167 149 161 113 115 102 130 151 144 101 154 105 132
153 115 116 151 139 64 145 134 145 117 115 149 155 134 100 109 144 161 101 161 168 123 116 153 140 101 112 144 155 151 150 100 162 102 116 163 104 153 104 135 97 151 170 153 143 144 151 142 162 110 164 117 144 143 108 151 137 118 145 145
155 163 155 148 110 128 104 114 77 112 147 166 101 166 104 156 104 141 136 155 105 154 134 100 111 137 114 153 147 149 147 149 117 145 149 153 132 116 173 116 101 116 151 151 108 142 143 162 152 114 137 172 162 148 115 163 159 64 167 147
162 112 148 168 153 171 128 104 166 151 156 110 116 111 147 160 147 114 102 147 149 110 134 151 117 137 145 160 162 130 101 166 141 137 64 155 155 152 165 111 162 162 64 163 142 101 101 156 162 138 147 150 152 110 146 139 76 116 156 141
101 115 149 146 155 132 145 105 162 154 115 114 134 154 141 103 157 151 147 76 102 153 154 148 99 139 157 173 116 148 152 110 153 155 152 64 161 139 100 115 167 139 150 154 148 149 151 138 109 110 165 115 105 158 150 170 150 152 105 149
104 152 111 147 147 115 156 154 134 114 148 138 64 163 154 137 101 159 109 100 143 147 151 115 140 101 167 156 148 114 149 111 164 157 145 97 157 151 149 154 117 148 148 99 135 101 161 146 105 151 128 115 97 155 158 103 149 160 109 105
149 148 154 101 166 157 109 134 160 161 129 76 105 135 99 154 148 114 135 152 156 155 101 161 159 108 149 156 138 64 151 157 152 116 144 164 102 164 146 64 154 151 147 151 101 99 158 155 110 168 154 158 76 101 170 159 148 147 115 138 157
134 105 158 162 171 101 166 155 101 119 143 152 153 141 126 110 150 152 161 169 132 110 155 104 139 114 154 150 110 155 104 141 97 139 114 147 144 168 64 146 143 152 165 103 168 102 101 145 148 163 155 154 97 160 111 104 149 134 166 121
105 154 105 150 141 115 118 139 143 157 116 145 148 117 160 104 153 114 149 152 149 165 121 116 146 104 130 145 162 101 163 156 116 151 102 116 156 141 101 118 159 150 155 152 147 110 161 113 113 150 151 151 105 156 134 118 153 111 115
164 112 151 149 160 137 110 116 154 138 110 168 104 147 162 163 147 100 134 153 97 157 150 152 116 115 162 161 140 140 64 132 165 168 148 157 108 144 148 116 167 116 101 97 147 133 114 168 144 113 64 164 148 110 142 147 156 104 176 101
155 146 64 154 164 138 145 135 158 142 99 159 111 116 156 141 105 149 157 101 149 156 97 171 97 170 101 111 169 153 147 162 140 114 162 172 161 126 101 143 153 152 152 126 105 130 127 64 142 170 101 165 113 114 136 123 117 155 154 101 160
111 167 117 154 145 116 137 161 116 130 144 157 115 167 116 101 97 145 147 110 168 137 136 157 111 143 142 64 156 148 105 155 154 138 147 116 105 152 156 115 164 147 157 152 137 64 144 148 144 142 141 157 156 121 123 117 160 111 152 101
142 168 115 116 148 142 103 141 160 114 149 138 143 166 167 101 147 102 115 154 156 156 171 134 158 115 145 145 111 147 155 147 114 108 143 150 164 97 157 157 162 110 99 144 158 148 115 167 144 108 98 134 114 147 168 129 110 146 125 114
98 158 168 127 64 150 153 160 163 163 153 105 134 166 64 144 152 101 103 160 151 151 121 113 120 147 144 163 159 141 118 146 97 153 157 171 134 155 161 64 163 142 101 110 149 156 167 161 147 113 64 157 150 101 105 151 162 101 159 146 150
155 147 116 97 161 139 64 163 153 155 149 152 78 115 168 154 148 110 140 146 162 115 114 163 154 101 119 144 150 101 152 147 97 144 132 105 167 156 152 64 151 152 116 139 172 142 146 159 101 111 157 105 170 145 101 151 162 148 64 174 138
155 140 104 157 110 154 137 153 117 135 157 138 150 148 64 136 163 144 102 124 110 116 145 147 115 150 164 149 141 99 163 143 111 162 116 101 104 138 130 150 153 140 64 138 154 115 116 138 138 101 144 111 172 162 108 138 152 108 173 104
136 111 163 161 157 168 154 149 167 142 152 121 98 154 110 141 116 167 104 137 105 158 138 144 138 114 133 147 150 144 142 166 152 106 116 124 112 145 160 137 110 168 145 136 101 162 110 149 167 64 168 154 134 99 152 167 114 156 138 116
161 123 119 111 154 142 165 151 164 168 147 151 112 64 157 150 101 109 152 160 164 101 162 138 147 160 115 103 158 156 101 166 150 150 152 110 155 120 111 131 147 112 64 147 152 111 170 141 101 116 161 138 116 101 159 145 140 155 157 153
64 171 144 114 115 148 139 107 116 154 138 102 154 147 138 109 142 156 116 167 116 101 97 166 158 114 163 148 115 64 149 163 149 115 155 138 150 109 148 162 171 97 151 130 129 103 159 156 105 151 144 101 109 135 158 140 121 101 123 115
116 145 153 64 155 151 151 134 121 115 116 151 139 64 135 111 152 146 156 114 104 166 166 118 156 141 138 146 140 151 64 148 148 116 149 150 167 157 134 165 116 156 110 97 162 140 101 112 166 148 152 151 156 149 155 151 115 103 165 134
152 157 101 147 102

RUNNING-KEY CIPHER

How do you recognise it?

If key is natural language:

- The cipher looks ridiculous and nothing like a natural language
- The ciphertext often has a flat frequency distribution. But with occasional spikes.
- Indicator blocks strewn throughout the text

RUNNING-KEY CIPHER

Method of breaking:

1. Shift common words past the ciphertext and look for readable words in the plain text
2. Use this seed word to gather more information by zig-zagging between plaintext and key
3. Find the source of the key, and the plaintext is found

If key is fully random:

If the key is not re-used the cipher is a one-time pad and perfectly secure

RUNNING-KEY CIPHER

Method of breaking:

1. Shift common words past the ciphertext and look for readable words in the plain text
2. Use this seed word to gather more information by zig-zagging between plaintext and key
3. Find the source of the key, and the plaintext is found

If key is fully random:

If the key is not re-used the cipher is a one-time pad and perfectly secure

RUNNING-KEY CIPHER

```
plain:   DEFEND THE EAST WALL AGAINST THE INVASION
plain:    THE THE THE THE THE THE THE THE THE THE
key:     IT WAS GROWING LATE IN THE AFTERNOON WHEN
cipher:  □□f□□□@□□□w□□□□tl□□□li□g□□□s□f¨□□n□□¤aª□□□□
```

RUNNING-KEY CIPHER

Method of breaking:

1. Shift common words past the ciphertext and look for readable words in the plain text
2. Use this seed word to gather more information by zig-zagging between plaintext and key
3. Find the source of the key, and the plaintext is found

If key is fully random:

If the key is not re-used the cipher is a one-time pad and perfectly secure

RUNNING-KEY CIPHER

```
plain:   DEFEND THE EAST WALL AGAINST THE INVASION
key:     IT WAS GROWING LATE IN THE AFTERNOON WHEN
cipher:  □□f□□□@□□□w□□□□tl□□□li□g□□□s□f¨□□n□□¤aª□□□□
```

RUNNING-KEY CIPHER

```
plain:   DEFEND THE EAST WALL AGAINST THE INVASION
key:     IT WAS GROWING LATE IN THE AFTERNOON WHEN
cipher:  □□f□□□@□□□w□□□□tl□□□li□g□□□s□f¨□□n□□¤aª□□□□
```

RUNNING-KEY CIPHER

Method of breaking:

1. Shift common words past the ciphertext and look for readable words in the plain text
2. Use this seed word to gather more information by zig-zagging between plaintext and key
3. Find the source of the key, and the plaintext is found

If key is fully random:

If the key is not re-used the cipher is a one-time pad and perfectly secure

BREAKING THE CODE

1. Introduction to Ciphers
2. Substitution Cipher
3. Permutation Cipher
4. Substitution & Permutation Cipher
5. Polyalphabetic Cipher
6. Periodic Polyalphabetic Cipher
7. Running-Key Cipher
8. Conclusion

CONCLUSION

None of these algorithms are inherently safe, but by making smart use of them and combining them together, you can make very secure encryption possible.

QUESTIONS?

ACKNOWLEDGMENTS

References:

http://en.wikipedia.org/wiki/Alberti_cipher_disk
http://en.wikipedia.org/wiki/Tabula_recta
http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
http://en.wikipedia.org/wiki/Polyalphabetic_cipher
http://en.wikipedia.org/wiki/Running_key_cipher
http://www.umich.edu/~umich/fm-34-40-2/ch8.pdf
http://www.umich.edu/~umich/fm-34-40-2/ch9.pdf
http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/7_Aperiodic
ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf