Information and Communication

Codebreaking for Traditional Cipher Systems

Abe Wiersma

UNIVERSITEIT VAN AMSTERDAM

26th January 2016

Table of Contents

- Introduction in Ciphers
  - Traditional Ciphers

- Breaking Traditional Ciphers
  - Substitution Cipher
  - Permutation Cipher
  - Permutation & Substitution Cipher
  - Poly-Alphabetic Cipher
  - Periodic Polyalphabetic Cipher
  - Running Key Cipher

- Modern Ciphers

Traditional Ciphers

- Origin lies in ancient Egypt $\sim$ 4000 years ago.
- Ends after second world war with the emergence of the computers.

Uses

- War movement.
- Government Secrets.

Types: Traditional Ciphers

- Substitution Cipher
- Permutation Cipher
- Substitution and Permutation Cipher.
- Running key Cipher
- An Enigma-style periodic poly-alphabetic Cipher

Introduction in Ciphers

- Traditional Ciphers

Breaking Traditional Ciphers

- Substitution Cipher
- Permutation Cipher
- Permutation & Substitution Cipher
- Poly-Alphabetic Cipher
- Periodic Polyalphabetic Cipher
- Running Key Cipher

Modern Ciphers

Substitution Cipher: Example

A Caesar Cipher is a Substitution Cipher that shifts a regular alphabet. Here a Caesar Cipher with a left shift of 3:

Plain:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:	XYZABCDEFGHIJKLMNOPQRSTUVW

Decoding a Caesar Cipher text with our Caesar cipher.

Ciphertext:

QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

Decoded Plaintext:

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Substitution Cipher: Problem

Substitution Cipher provided by Mathias

```
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 ; 8
WP8EPHRRWA1 ; 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  8
Z1HP8EPZRV8YI1 ; 8 : ; H1HP8VRZP19RPO8ZYWCP9LWPELYYR : P ; : PLI1IS : CP19RP  LHH ; 8 : HPO9 ;
N9P9LWPN8 : VIYHRWPSL : T ; : WPORZRPNZIH9RWPE8ZP19RP1 ; SRCPL : WP19RP1Z ; IS   9
HP8EPWRS8NZLNFPORZRPLZZRH1RWDPLP1RZZ ; 7YRPZRLN1 ; 8 : P9LWPHR1P ; : QPRX  RZ ; R :
NRP8EPHIEERZ;: – P9LWPW8 : RP ; 1HPO8ZTQPL : WPHO ; E1PLHP19RPH9LWRHP8EP:; – 91
P7RE8ZRP19RPZLFHP8EP19RPLHNR : 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
```

Substitution Cipher: Solution

Finding the solution is a process of small increments.

Analysis of the Cipher text gives us the number of different characters: 35

And also gives us the frequencies of the characters →

Character	Frequency in %
p	16.86
r	10.83
1	6.723
;	6.296
l	6.083
h	5.869
:	5.763
8	5.336
z	5.336
9	4.268
w	3.361
y	3.201
i	2.401
e	2.401
n	2.187
s	1.867
	1.814
f	1.440
o	1.387
-	1.334
7	1.334
c	1.173
v	0.907
d	0.640
t	0.266
x	0.213
q	0.213
a	0.106
.	0.053
,	0.053
k	0.053
b	0.053
u	0.053
g	0.053
m	0.053

Substitution Cipher: Solution

A space is the most common character in the English language, which implies p decoded is ' ‘

We can also apply that the most common letter in the English language is the letter e, which implies that r decoded is 'e‘

Substitution Cipher: Solution

Substitution Cipher provided by Mathias

```
evezf19;:– :8o –8eh 8: l1 19e –lyy8 d 19eze ;h l zl;yolf h eew ;: 19e h1;zz;:– 8
e 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 19
l1 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 7
f 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
```

Substitution Cipher: Solution

So this intermediate step contains a lot of 19e, and the is the most common trigram in the English language. 19e decoded is the.

Substitution Cipher: Solution

Substitution Cipher provided by Mathias

```
evezfth;:— :8o —8eh 8: lt the —lyy8 d theze ;h l zl;yolf h eew ;: the ht;zz;:— 8
e the s;:wc :8t yehh thl: ;: the s8vese:t 8e the 78w;eh 8e se:d the h8n;ly l:w
8y;t;nly  lhh;8:h hlve lnmi;zew hinh ;:te:h;tfc l:w 7ee: h8 o;weyf w;eeihewc
thlt the;z ;:ev;tl7ye zehiyth lze lys8ht ;ssew;lteyf  z8winewd the  ez;8w 8e
heewat;se l:w hlzveht hlh 7en8se lh hh8zt ;:  8y;t;nly lh ;t ;h ;: l—z;niytizly
yl78izd l h;:—ye felz 7z;:—h ;th l  z8 z;lte ezi;th t8 sltiz;tf ;: the s8zly lh
;: the  hfh;nly o8zywd e;—htf felzh eyl hew ;: z8se ez8s the t;se ohe: the  8y;t
;nly  lhh;8:h oeze e;zht ht;zzew 7f t;7ez;ih —zlnnhihc 7ee8ze ;th i:ziyf n;t;ke:
h oeze e;:lyyf hi7wiew 7f the lztc 8z wen;sltew 7f the nzieytf 8e 8ntlv;ihd e:—
yl:w i:wezoe:t h;x felzh 8e n;v;y olz l:w hieeez;:—c 7ee8ze the ls7;t;8: l:w slw
:ehh 8e the y8:—  lzy;lse:t oeze ex eyyew 7f the  iz—e 8e  z;wec 8z nzihhew 7f
the ho8zw 8e nz8soeyyb toeyve felzh eyl hew 7etoee: the n8:v8nlt;8: 8e the
htlteha—e:ezly ;: ,u.gc l:w the ext;:nt;8: 8e the y;ne:he 8e the eze:nh zev8yit
;8: 7f the lzs 8e :l 8ye8:d 7itc 8: th;h 8nnlh;8:c ;: 8:e felzc lyyc ;: the sel:
t;se lt yelhtc hlh 7ee: lnn8s y;hhewd eze the yelvehc oh;nh i:e8ywew ;: h z;:—
ls;wht the 8vezthz8o 8e thz8:ehc l:w the tzl:h 8zth 8e zev8yit;8:;hth 8vez the
o8zywc hlw elyye: ;: litis:c the  lhh;8:h oh;nh hlw n8:viyhew sl:t;:w oeze
nzihhew e8z the t;sec l:w the tz;is hh 8e wes8nzlnf oeze lzzehtewd l tezz;7ye
zelnt;8: hlw het ;:q ex ez;e:ne 8e hieeez;:— hlw w8:e ;th o8ztq l:w ho;et lh the
 hhlweh 8e :;—ht 7ee8ze the zlfh 8e the lhne:w;:— hi:c hlw w;hl  elzew the eezse
:t 8e zev8yit;8: 7ee8ze the lz8ihew ;:w;—:lt;8: 8e the i:n8zzi tew  lzt 8e sl:t
;:wd the hlse  lhh;8:h slf l—l;: lz;heq the hlse weyih;8:h l—l;: h zelwc lh h;:
h z;:—h i  lezehh ;: hinnehh;ve —e:ezlt;8:h 8e se:q 7it oe t:8o the zehiytd thef
 o;yyc y;te the olfh 8e the i:z;—hte8ihc 7e l—l;: nzihhewd
```

Substitution Cipher: Solution

From here words start to be distinguishable, and with the help of a English letter frequency table this is the result.

Substitution Cipher: Solution

Substitution Cipher provided by Mathias

```
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.
```

Substitution Cipher: Solution

Plain: abcdefghiklmnopqrstuvwxyz ,-.1789:;
Cipher: -:,.fy9suzaqcwp;rmk7vdxlrp1g8tbohni

BLACKWOOD'S MAGAZINE, Jan. 1845

Substitution Cipher: Solution

- All frequency properties of the underlying language remain intact.
- Thus are breakable by statistical frequency analysis

Introduction in Ciphers

- Traditional Ciphers

Breaking Traditional Ciphers

- Substitution Cipher
- Permutation Cipher
- Permutation & Substitution Cipher
- Poly-Alphabetic Cipher
- Periodic Polyalphabetic Cipher
- Running Key Cipher

Modern Ciphers

Permutation Cipher: Example

A Permutation Cipher is a Cipher that scrambles characters of plaintext in blocks of a fixed length.

Plain:	This is a test
Cipher:	iis hTs stea t

Blocks of 7 characters in length.
Key to decrypt: 5406312

Permutation Cipher: Problem

Permutation Cipher provided by Mathias

```
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
```

Permutation Cipher: Solution

Solution

Permutation Cipher: Solution

Permutation Cipher provided by Mathias

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.

Permutation Cipher: Solution

- 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.

Introduction in Ciphers

- Traditional Ciphers

Breaking Traditional Ciphers

- Substitution Cipher
- Permutation Cipher
- Permutation & Substitution Cipher
- Poly-Alphabetic Cipher
- Periodic Polyalphabetic Cipher
- Running Key Cipher

Modern Ciphers

Permutation & Substitution Cipher: Problem

Permutation & Substitution Cipher provided by Mathias

```
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?AJ!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
```

Permutation & Substitution Cipher: Solution

Again finding the solution is a process of small increments.

Analysis of the Cipher text gives us the number of different characters: 35
And also gives us the frequencies of the characters →

Character	Frequency in %
J	17.70
I	10.25
Z	6.642
’	6.496
T	5.985
F	5.802
?	5.620
U	5.583
Q	5.364
”	4.525
!	4.379
.	2.445
X	2.226
S	2.189
A	1.970
D	1.897
O	1.642
M	1.569
L	1.532
-	1.423
K	1.204
V	1.058
W	0.620
B	0.620
P	0.291
C	0.218
E	0.182
R	0.109
Y	0.109
H	0.072
;	0.072
G	0.072
,	0.036
	0.036
N	0.036

Permutation & Substitution Cipher: Solution

A space is the most common character in the English language, which implies J decoded is ' '

We can also apply that the most common letter in the English language is the letter e, which implies that I decoded is 'e'

Permutation & Substitution Cipher: Solution

Permutation & Substitution Cipher provided by Mathias

```
QU Tt QG?Det UOUtQ?QtS’?.t ’—!Fe!T F?” —QU T eUF!. E?Q”D U”FO’tTtU?tD  L?FU. O—FeT!t!!eeS —FM’
 AeT—t ?t!Q  ”’et.  ’..Tte !TS’Q  WUX’Tte F?eFA AUet e!eL  MTeFFULB?SQe? U?Ft!t T”et Tt?D e—eL ’e!
t ’eFQU T Tte?. Qt;!?AP ’FeG e—!MUO”? T .Fe’S”e QQt? TtD ?tUeT  Q ’TTDQ t”?Fe X’ eATt—e F’ t’O’
SQ’ .Q; ttER ’K ”DF? FteT —!eT!OFte MT”e?DQ e!O!Q ”FeO’—K  ” XtX?K ’eT MDQ—D e’TO Ve!U?”!K L?FUt
 ?”FUtFFOUTA LtUTD QU T XX?UB WT—F’ DQU!.U FQ” Fe ’D’t e?!eFUQ?LUTA tF?” E!.’ MTQ? A? FeAL?U ”Ut
’?t.’  F”FMUA eXT eP”’’Q’tA e!tD ”eXTSU tW— QUU Q’QVAeX KU” e’tU!KSQTte eeSFQ TDU eF ’TS’t’ DXV?
 PU FeSeT t ’T’SQ’!’YXT eWAM— !FQ’eTDFU”A Q? D UXee! ”.eB At’!” eeTQeQ!V F’’UQ?USS”e F’t T—K”
UQU?!SLQXO .e!?LTSD ?Me?S! QeQ”Qe”F ? LF!’SXO?t? ”KetBee —K ’—!FU  — eQTt’’XTS!AQ W?T! W QPU!eQ”
QUAU T e.S.?F’?Ut—XMet”F ? ”U ?Q e.TQ tSXeU.”F’ t’FeUTQ .FF’U SFeeS’!A. eT t Q!tU.F?” M”? T eB!
eFQeV” e!”U? .U’ K eQt LAFU ee”?e”FUBH OWtF??UX”F ? ,U?Xe!eeD QX’? ’AF?  ttQL. UeT ttQ!eKQ ’ Dt’
t!U eT!V’V?Ut’?KVO’ FUTQ FF’”S Wt SO!’LeLF?” etUtX F eeXeD! ”e”X etTeLUeK— ” ”AF’OQ!?e’t  e eteQ
!U eTeUF!.F’S ”’A! e?A” e?TV e M?—VT ’”F ”QeV Ft’’?TB ’UTA e Qt? S TeT .UeUTte F— ’!U.TOtOVQ’
XWQ t! tUOK?DQ t!? . ..eU”tF e!Tt UDeeF!LD TMe’FD ’Xet. XX ?  eDTtStTe!eFQ”e.’  Q eSF’UBSF’ ”’
 etTte . M?t.” e”FtSeetFU  ”eQX?Kt?t —UTFS?Tte LQUL” eS.?!S TXOeL !?? F’tFF’U tF eS ”VF?QUe?!t!T’
D?X” —eT  W ”t?TFe P? QQUT t??eTte ttR!e tU—Ae .t’ Q SeTX’Y’TA’M’!”F ?  QT?DFUL”UQU T eS ?.T UFU
?TF Q E?Q”t T”FTL O’’K— ? .D’ e”!F’ XQO.U!tUVF?” Q!t’Q F eLFMe B! QF?DK ?D’”e Ttt eFUMQ !? ”QF?
UKFK’X?’ L W””OT ?W!QUM!!’T D  ”K?T FLeeFULBUAU T eB! ?eQB — eX!eOt!SeQ tMe XQXU”’ ’t!e B’MA UT!
VeAUFULQQ’VFO AU T  eFTtQeQSe —’tUe!t .FUL!UtF’U QU T A’M’! ’Qt  P.ee AL’!t T”’. ’t?BUeL!QQ eFV
!FU!e —? ”!F?FetVeeSMF?UTSD T eMT’’ t TS OA!?ee.D ’M” ”FXOK et’Q?Ue ’ K—XFUe?t!.’ ”UTQ A..e’ ”e
”F ””F?OLQQU ”Qet’’XTSXeX.YWQ D’F ’eTt TMD.e’!e M?e!eQM’!”F ? e” ?A QDUTt ’—?”!Q?DeT t !’M’” F”U
 LF U’SUTTD eTT ? L”? FtU?FeS ’tFeO’Tte !eRSe Ut’?!? FQF’VU ””e tFLFeU.’ .Q!eT t Q—M’K’T D eU”!
SQ?  MV ?eT”e QQAeMTt’LMC ’TOt UTet  C? ..  ’”FD’eXXUTA ”tFUO Tte X?QD —AU T et!FeeT t QOe’TeTF W
 MT—!BeeD’D ?M!Tte QXF—’ ”? X  ’”TDF ’”UVOK t”U ?!EA UTM!  ’.O’LTt!Le T eTFeK e”?eB”?T FQU U”Q ’S
?e!L X?O.F?FA t ’!e”!Q?DAUMT  eST ”X O’ tK’F. etO” UXee!QtQ ”teQeQe ’AU T eV?V?X?A ! tKQ’ePF’!!?
teT WT”etQU e! eXXKAeeAM” e!t TFUUA” e’ .tQQU T M— ’Ht? Tt t?OKDe . !OQ’T”? T V?QXeQ U”e eTSFe.X
 eX?X teT t teS!DF”eeT’ .QQeF ’ VV’OQ ”teQeK  ’XUtOL.’  —.etTtDCT Wt Tt?CM FeQ ?eTt ’”UAUQT M.
XeQOtAC etK . eeTFULXe.’  Q ADUTQ t’TQ” F?BFU’S”e tSt T.’!SU e M?eAt T”F.e’!eT ?e!’Ft QeT t QFS’
SQOF’U Q’QeFUF .FeSS’’t  eVV’OQT Ut!U  NAFF’?SU.F tFU  ”T e—A tt!?VOK ’”U ?!MACUT eQT M” U?T eQ
?’’Pt ’e!L ? FeLeF” ” —tK T ?eT? F”FeX” ”eTAt !S’? t TQQ?XD e   WF
```

Permutation & Substitution Cipher: Solution

Solution

Permutation & Substitution Cipher: Solution

Permutation & Substitution Cipher provided by Mathias

```
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
```

Permutation & Substitution Cipher: Solution

From here we start filling in letters, like tTe→the. With the help of a English letter frequency table and knowledge of the English dictionary, word by word you get the solution.

Permutation & Substitution Cipher: Solution

Permutation & Substitution Cipher provided by Mathias

```
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 made 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 looded most wretchedly. it is impossible to describe the scene which now
tood 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
dissed him affectionately, and said she felt confident of his innocence from the first, and had
never despaired of its being made evident. Huliana and eli,a 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 taden 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 seed 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 brodenhearted. he still remembered, in the midst of his Hoy, 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 tood george and ned by the hand and led them across the lawn.
```

Introduction in Ciphers

- Traditional Ciphers

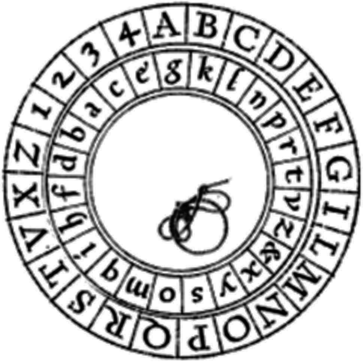
Breaking Traditional Ciphers

- Substitution Cipher
- Permutation Cipher
- Permutation & Substitution Cipher
- Poly-Alphabetic Cipher
- Periodic Polyalphabetic Cipher
- Running Key Cipher

Modern Ciphers

Poly-Alphabetic Cipher: Alberti cipher

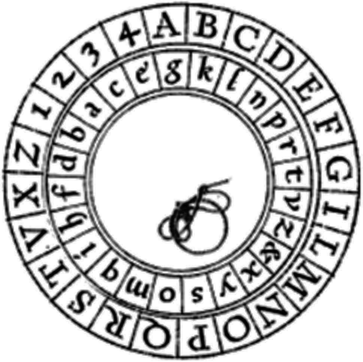
'First' known use:
Leon Battista Alberti $\sim$ 1467
Works by:
Using multiple alphabets to encode plain text
Switches alphabets after one or more words


A B C D E F G I L M N O P Q R S T V X Z 1 2 3 4
g k l n p r t v z & x y s o m q i h f d b a c e

Poly-Alphabetic Cipher: Alberti cipher

Stationary disk
ABCDEFGILMNOPQRSTVXZ1234
Movable disk
gklnprtuz&xysomqihfdbace

Plaintext:
LAGVERRA...
Ciphertext with index g:
AzgthpmmgQ...


A B C D E F G I L M N O P Q R S T V X Z 1 2 3 4
g k l n p r t u z & x y s o m q i h f d b a c e

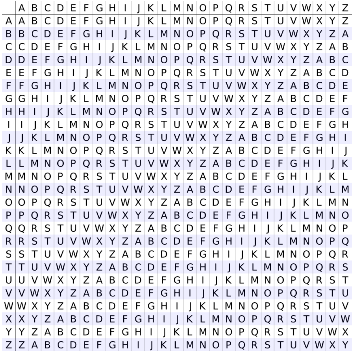
Poly-Alphabetic Cipher: VIGENÈRE CIPHER

Invented by:

Giovan Bellaso ∼ 1553

Works by:

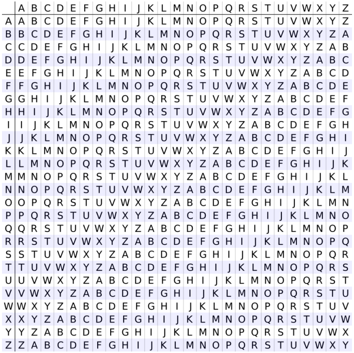
- Using a key with a polyalphabetic cipher.
- Switching alphabet with the key every character.
- Keep repeating the key over the plaintext.



	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

Poly-Alphabetic Cipher: VIGENÈRE CIPHER

Plaintext:
THEWARSTARTS...
KEY=BANANA:
BANANABANANA...
Ciphertext:
UHRWNRTTNRGS...



	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

Introduction in Ciphers

- Traditional Ciphers

Breaking Traditional Ciphers

- Substitution Cipher
- Permutation Cipher
- Permutation & Substitution Cipher
- Poly-Alphabetic Cipher
- Periodic Polyalphabetic Cipher
- Running Key Cipher

Modern Ciphers

Periodic Polyalphabetic Cipher:

Properties:

The frequency distribution is completely flat

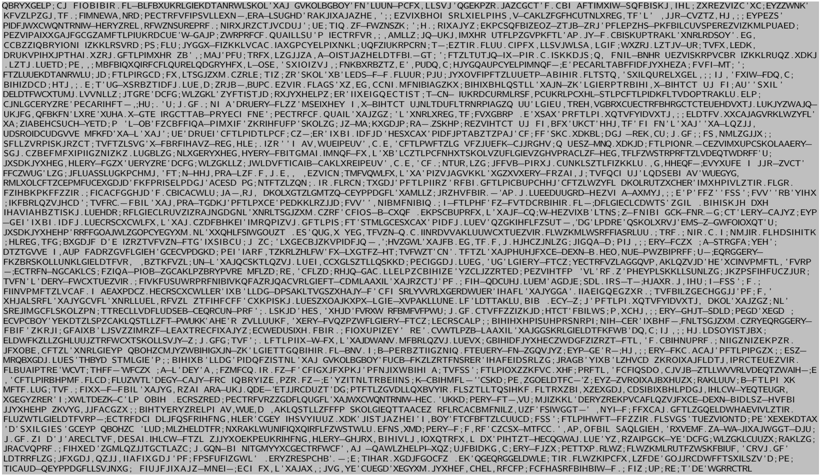
Decoding:

Search for repeating patterns in the ciphertext

Get the distance between these patterns, and calculate the greatest common divisor.

Periodic Polyalphabetic Cipher: Problem

Periodic Poly-Alphabetic Cipher(like Enigma) provided by Mathias



```
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 SRLYVVRLXGERDWUER'IHAFL'XAJYGGA'. IIAEIGQEGZXR. ; TVFBILZGECHGGJJ'PF; F, '
XHJALSRFL'XAJYGCVFL'XNRLLUEL, RFVZL ZTFIHFCFF'CXKPISKJ. LUESZXOAJKXPX—LGIE—XVPAKLLUNE. LF'LDTTAKLU, BIB . ECY—Z; J'PFTLPI. XQTVFYIDVXTJ, DKOL'XAJZGZ; NL'
SREJIMGCFLSKOLZPN; TTRECLLVDFLUDSEB—CEQRCUN—PRF'; . LSKJD'HES, 'XHJD'FVRXW RFBMFVFPWU; J. GF. CTVFFZZIZKJD; HTCT'FBILWS; P, XCHJ, ;; ERY—GHJT—SDLD; PEGD'XEGD ;
ECVPCBOY'YEKDTZLSPZCAKLQSTLLZFT—PWUKK'AHE'R ZVLLUUKF, 'XERY—FVQZPZWFLGIERY—FTCZ; LECRSCALP; ; BIHIHXHPISUHPRSNRPI; NIH—CER'IXBHF—, FNLTSGJZXM. CZRYEQRGGERY—
FBIF'ZKRJI; GFAIXB'LJSVZZIMRZF—LEAXTRECFIXAJYZ; ECWEDUSIXH. FBIR. ; FIOXUPIZEY' RE'. CVWTLPZB—LAAXIL'XAJGGSKRLGIELDTFKFWB'DQ, C; IJ, ;; HJ. LDSOYISTJBX;
ELDWFKZLLZGHLUUJZTRFWCXTSKOLLSVJY—Z; J. GFG; TVF'; . LFTLPIIX—W—FX, L'XAJDWANV. MFBRLQZVJ. LUEVX; GBIHIDFJYXHECZWDGFZIZRZT—FTL, 'F. CBIHNUPRF. ; NIIGZNIZEKPZR.
JFXOBE, CFTZL'XNRLGIEYP QBOHZCMJYZWBIHIGXJN—ZK'LGIETTGQBIHIR. FL—BNV. I; B—PERBZTIIGZNIQ. FTEUERY—FN—ZGQVJYZ; EYP—GE'R—; HJ, ;; ERY—FKC. ACAJ'PFTLPIPGZX; ; ESZ—
MRQBXGDJ. LUES'THBYD STMLGIE'P; ; BIHIXB'LLDG'PIDQFZISTNL'XAJ GVKOLBGBOY'FUCB—FKZLZRTFNSRER'IHAFEIDSRLZG; JRAGB'YIXB'LZHVCD ZKROIXAJFLDTJ, IPRCTEUEZVIR.
FLBUAIPTRE'WCVT; THFF—'WFCZX ; A—L'DEY'A, ; FZMFCQ. IR. FZ—F'CFIGXJFXPKJ'PFNJIXWBIHI A; TVFSS'; FTLPIOXZZKFVC. XHF; PRFTL, 'FCFIQSDO, CJVJB—ZTLLWVVRLVDEQTZWAIH—; E
, 'CFTLPIRBHPMF. FLCD; FLUZWTL'DEGY—CAJY—FRC IQBRYIZE, PZR. FZ—; E'YZITNLTRBEIINS; K—CBIHMFL—''CSKD; PE, ZGOELDTFC—'Z; EYZ—ZVROIXAJBXHUZX; RAKLUUV; B—FTLPI XK
MFTF. LUG; TVF. ; FIXX—F—FBIL'XAJYG, RZAI ARA—UKJ. QDE—'ETJJRCDUZT'DG; PTFTLZGVDLLQXBVYIR. FLSZTLLTQSIHKF. FLTRXZBI, XZEXGDJ, CDSIBIXBHLPDGJ, IHLCW—YEQTEUGR,
XGEGYZRER'I; XWLTDEZK—C'LP OBIH . ECRSZRED; PECTRFVRZZGDFLQUGFL'XAJWXCWQNTRNIW—HEC. 'UKKD; PERY—FT—, VU; MJIZKKL'DERYZREKPVCAFLQZVJFXCE—DEXN—BIDLSZ—HVFBI
JJYXHEHP ZKVYG, JJFACGZX; ; BIHTYERYZRELPI AV, WUE, D , AKLQSTLLZFFFP SKOLGIEQTTAACEZ RFLRCACBMFNILZ, UZF'FSIWGGT—' , NYI—F; FFXCAJ. GFTLZGQELDWHAEVIVLZTIR.
FLUZWTLGIELDTFVRP—; ECTRFDCI DLJFQSFRIHFNG, HLER'CGEY IHSVYIUUZ. XDK'JISTJAZHEI'I, BOY'FTCFBFTZLCUUCD; FSS'; FTLPIHWFT—FFZZIR. FLSVGS'TUEZVIONTD; PE'XEXEKDTAX
'D'SXILGIES'GCEYP QBOHZC 'LUD; MLZHELDTFR; NXRAKLWUNIFIQXQIRFLFZWSTWLU. EFNS, XMD; PERY—F; F, RF'CZCSX—MTFCC. ' , AP, OFBIL SAQLGIEH, 'RXVEMF. ZA—WA—JIXAJWGGT—DJU;
J. GF. ZI D'J'ARECLTVF, DESAI. IHLCW—FTZL ZJJYXOEKPEUKRIHFNG, HLERY—GHJRX, BIHIVLJ, IOXQTRFX, L DX'PIHTZT—HECQGWAJ. LUE'YZ, RZAIPGCK—YE'DCFG; WLZGKLCUUZX; RAKLZG;
JRACVQPRF. ; FIHXED'ZGMLQZJJTGCTLAZC; J. GQN—BI NITGMYYXCGECTRFWCF' , AJ —QAWLZHELPI—XQZ; UJFBIDKG, C; ERY—FJZX; PETTXP. RLWZ; FLWZKMLRUTFZWSKFBIUF, 'CRVJ. GF'
LDTRRFLZG; JFXGDJ, QZJJ, IIAFIXGDJ'PF; FPSFUFIZGWL' . ERYZRESPCHB'.—; E; TIHAR. XGDJFGOCFZ . EK'QGEQRGGELDWLE; TIR. FLWZKIPCFX, LZFDE'GOJJRCDWFFTSXILSZV'D; PE;
TICAUD—QEYPPDGFLLSVJNXG; FIUJFJIXAJZ—MNEI—; ECI FX, L'XAJAX, ; JVG, YE'CUEGD'XEGYXM. JYXHEF, CHEL, RFCFP; FCFHASRFBIHBIW—F. ; FIZ; UP; RE; T'DE'WGRRCTRL
```

Periodic Polyalphabetic Cipher: Solution

Introduction in Ciphers

- Traditional Ciphers

Breaking Traditional Ciphers

- Substitution Cipher
- Permutation Cipher
- Permutation & Substitution Cipher
- Poly-Alphabetic Cipher
- Periodic Polyalphabetic Cipher
- Running Key Cipher

Modern Ciphers

Running Key Cipher: Example

Running Key Cipher: Problem

Running Key Cipher: Solution

Modern Ciphers

- Private-key cryptography, where the same key is used for encryption and decryption.
- Public-key cryptography, where two different keys are used for encryption and decryption.

Ciphers can be distinguished into two types by the type of input data:

- Block ciphers, which encrypt block of data of fixed size
- Stream ciphers, which encrypt continuous streams of data

Stelling

Theorem (Massa-energierelatie)

$E = mc^2$

Conclusie

Belangrijkste conclusie