

Information and Communication
Codebreaking for Traditional Cipher Systems

Abe Wiersma



UNIVERSITEIT VAN AMSTERDAM

1st February 2016

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

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

Uses

- ▶ War movement.
- ▶ Government Secrets.



- ▶ 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: ABCDEFGHIJKLMN**OP**QRSTUVWXYZ
Cipher: XYZABCDEFGHIJKLMN**OP**QRSTUVWXYZ

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;  
EEIHRWC19L1P19R; ZP;: RV; 1L7YRPZRHIY1HPLZRPLY8H1P; SSRW; L1RYFP Z8WINRWD19RP RZ; 8  
WP8EPHRRWA1; SRPL: WP9LZVRH1P9LHP7RN8SRPLHHP98Z1P;: P 8Y; 1; NLYPLHP; 1P; HP;: PL-Z;  
NIY1IZLYPYL78IZDPLPH;: - YRPFRLZP7Z;: - HP; 1HPL Z8 Z; L1RPEZ1; 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;: LYFPHI7WIRWP7FP19RPLZ1CP8ZPWWRN;  
SL1RWP7FP19RPNZIRY1FP8EP8N1LV; IHDPR: -YL: WPI: WRZOR: 1PH; XPFRLZHP8EPN; V; YPOLZPL:  
WPHIEERZ;: - CP7RE8ZRP19RPLS7; 1; 8: PL: WPSLW: RHHP8EP19RPY8: -P LZY; LSR: 1PORZRPX  
RYRW7FP19RP IZ-RP8EP Z;  
WRCP8ZPNZIH9RWP7FP19RPHO8ZWP8EPNZ8SORYYBP1ORYVRFRLZHPRYL HRWP7R1ORR: P19RPN8:  
V8NL1; 8: P8EP19RPH1L1RHA-R: RZLYP;: P, U. GCPL: WP19RPRX1;: N1; 8: P8EP19RPY; NR:  
HRP8EP19RPEZR: N9PZR8YI1; 8: P7FP19RPLZSP8EP: L 8YR8: DP7I1CP8: P19; HP8NNLH; 8: CP;: P8:  
RPFRLZCPLYCP;: P19RPSRL: 1; SRPL1PYRLH1CP9LHP7RR: PLNN8S Y; H9RWDPRZRP19RPYRLVRHCPO9  
; N9PI: E8YWRWP;: PH Z;: - PLS; WH1P19RP8VRZ19Z8OP8EP19Z8: RHCPL: WP19RP1ZL: H 8  
Z1HP8EPZRV8YI1; 8;: H1HP8VRZP19RPO8ZYWC9LWPELYYR: P;: P L1I1S: CP19RP LHH; 8: HPO9;  
N9P9LWPN8: VIYHRWPSL: T;: WPORZRPNZIH9RWPE8ZP19RP1; SRCPL: WP19RP1Z; IS 9  
HP8EPWRS8NZLNFOPZRPLZ8RH1RWDPLP1RZZ; 7YRPZLN1; 8: P9LWPHRP1;: QPRX RZ; R:  
NRP8EPHIEERZ;: - P9LWPW8: RP; 1HPO8ZTQPL: WPHO; E1PLHP19RPH9LWRHP8EP;: - 91  
P7RE8ZRP19RPZLFHP8EP19RPLHNW;: - PHI: CP9LWPW; HL RLZRPW19RPERZSR: 1P8EPZRV8YI1; 8:  
P7RE8ZRP19RPLZ8IHRWP;: W;: -L1; 8: P8EP19RPI: N8ZZI 1RWP LZ1P8EPSL: T;: WDP19RPHLSRP  
LHH; 8: HPSLFPL-L;: PLZ; HRQP19RPHLSRPWRYIH; 8: HPL-L;: PH ZRLWCPLPH;: 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.

Character	Frequency in %
p	16.86
r	10.83
l	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
.	0.053
k	0.053
b	0.053
u	0.053
g	0.053
m	0.053

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

And also gives us the frequencies of
the characters →

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;NIY1ZLY
YL78IZD L H;:-Ye FeLZ 7Z;:-H ;1H L Z8 Z;L1e EZI;1H 18 SL1Z;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;1H -ZLNN9IHC 7eE8Ze ;1H I:ZIYF N;1;
Ke:H OeZe E;:LYYF HI7WleW 7F 19e LZ1C 8Z WeN;SL1eW 7F 19e NZLeY1F 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:V8N1L;8: 8E 19e
H1L1eHA-e:eZLY ;; ,U.GC L:W 19e eX1;:N1;8: 8E 19e Y;Ne:He 8E 19e EZe:N9 ZeV8Y11
;8: 7F 19e LZS 8E :L 8Ye8:D 711C 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 ZeV8Y11;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;1S 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 ZeV8Y11;8: 7eE8Ze 19e LZ8IH8e ;;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 711 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 these ;h l zl;yolf h eww ;: 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 lnm;zew hinh ;:te:h;tfc l:w 7ee: h8 o;weyf w;eeihewc
thlt the;z ;:ev;t17ye 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:wezoet h;x felzh 8e n;v;y olz l:w hieez;—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 7etoe: the n8:v8nt;8: 8e the
htlthea—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:e8yew ;: 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 hieez;— 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 eeze
: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 weyh;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 HORTWMM NNTEO COG FNDIHN TIR ETATSE HHICW, T
NOS I BEO TEECTFEFHY TBD SEANME ICHH VN COETHITUTISTEITS ON HAS
LFEVIDOPRSTHI D.CNVIO CLN, OTIP IMGON SEDSREHN TOUPOATINE AND N,OERWTIN
ASNVEEWER ITTTH I WYWER HEWAMER F OFKORI BRETHIH MSTIV HA,NDM COGINOO CTE
IDECINHH TTWIIASSPE C INSONTNT EIDYARTPO IVISI D INSON REEFA TE,AST
INSHASCESOPRM TIF OUODPE 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 HAENMGOCBE 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 NTUNEORRRFIT S, ,OWSLOLN A S ARSSAEECEONSCY ,
NCEEQUAT H TNMAI HETFORF EHF TOS YARTPE EPOSP ODO ATD RISTNMIAN IATHYS ALWE
BEEAVCSIN N,SHE TE SRESPUP OFNIOB REETH IONLEL5174 INFO ET, WT, CFE
INNHETISOPOP , ANIO NGEACHEGEN INI OPLRAAN, ONIE WH,NDON PIN O, TRWE RRYA CHT
CATHNE IGANEFF TOABY CTEANGH CL POF OH. TYICLLD OE NOF AWIRE UATLTLISS E
OPN I.IONTRANTIOC AED RN A IONTACAE MLRU ND;INK INDANF EFETHFS OTORERTIA
PAUTUMS TOYLLNPLASU 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 block sizes this is pretty hard, but then one can probably solve anagrams within the block size which also reveals the key and block size.

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' - I FI ! TJF?' J - QUJTJIUF ! , JE?Q'DJU'FO'ZTZU?ZDJJL?FU, JO - FIT ! Z !! IIS J - FM'
 AIT - ZJ?ZIQJ'' IZ , J' . , TZIJ ! TS' QJJWUX' TZIJF? IFAJAUZJ ! I ! LJMTIFFULB?SQI?JU?FZ ! ZJT' IZJTZ? DJI - I LJ ' ! I
 ZJ' IFQUJTJZT? , JQZ ; ! ? APJ' FIGJI - MUO'' JTJ , FI ' S' ! IJQZQ?JTZDJ?ZUITJJQ' TTDQZ?'FIJX'JIATZ - IJF'JZ' O'
 SQ' J , Q; JZZERJ' KJ'DF?JFZITJ - IIT ! OFZJMT' I ?DQJ ! OIQ' FIO' - KJJ'JXZX?KJ'ITJMDQ - DJI' TOJVI ! U?' ! KJL?
 FUZJ?'FUZFFOUTAJLZUTDQJQJTXJX?UBJWTF - JDQU ! , UJFQ' FFIJ ' D' ZJ ? ! IIFUQ?LUTAJZF?' JE ! , 'JMTQ?JA?JFIAL?UJ
 "UZ'Z , ' ' JF' FMUAJIXTJIP' ' ' Q' ZAJI !ZDJ'IXTSUJZW - JQUUJQ'QVAIXJKU' JI 'ZU ! KSQZTJIIISFQJTDUJIFJ' TS' Z'
 JDXV?JP.UJFISITJZ' T' S'Q' ! 'YXTJWAM - 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' - IFUJ - JIQTZ' 'XTS ! AQM?T ! JWJQPU!
 IQ"QUAUZTJI, S. ? F?UZ - XMIZ'FJ?J'UJ?QJ, TQJZXSXIU , 'F'JZ'FIUTQJ, FF'UJSFIIS' ! A, JIJZJQJ !ZU, F?'JM'?
 JIJB ! IFQIV' JI ! 'U?J, U'JKJIQZJLAFUJII' ? I' FUBHJOWZF?'UX'FJ?J, U?XIIIDJQX' ? J'AF?JJZZQL, JUITJZZQ!
 IKQJ'JZ'Z ! UJIT ! V'V?UZ?'KVO'JFUTQJFF' " SJWZJSO ! 'LILF?' JIZUZXFJIIIXD ! J' ! "XJIZTILUIK - J" J'AF' OQ ! ? !'
 ZJJIJIZIQ ! UJITIUF ! , F' S'J' 'A ! JI' ? TVJIJW' - VTJ' ' FJ' QIVJFZ' ? ? TBJ' UTAJIJQZ? JSJTIJ, UIUTZIJF - J' ! U,
 TOZOVQ'JXWQZJIZUOK?DQJZ ! J, J' , 'U'Z'FJ ! TZJUIDI ! LDJTM ! 'FDJ'XIZ, JXXJ?JJDZS2T ! IFQ' ! , 'JJQJIS' !
 UBSF' J' ' IZTZIJ, JM?Z, ' JI' FZSIIFUJ' 'IQX?KZ?ZJ - UTFS?TZIJLQUL' JIS, ? ! SJTXOILJ ! ? ? JF'ZFF'UJZJFISJ'V?F'
 QUI? ! ZIT'D?X'J - ITJWJ'Z?TFIJP?JQUTJZ?ITZIJZR ! IJZU - AIJ, Z' JQSITX'Y' TAM' ! ' FJ?JQ?T'DFUL'
 UQUJTJISJ', TJUFU?TFJQJ?Q'ZJT'FTLJO' 'K - J?J, D' JI' 'IF'JXQO, U !ZUVF?'JQ ! Z' QJFJILFMIJB ! JQF?DKJ?D" "
 IJZZZJIFUMQJ ! ? J'QF?UKFK'X' 'JLJW' " OTJ'W ! QUM ! ! 'TJDDJ"K?TJFLIFULBUAUJTIJB ! J ! IQB - JIX ! IOZ !
 SJZMIJXQXU' " J'Z ! IJB' MAJUT ! VIAUFULQQ' VFOJAUJTJFIFTZQIQSJJ - ZUI ! Z', FUL ! UZF' UJQUJJA' M' ! J' QZJJP,
 IJAL' ! ZJT' ' , J'Z?BUIL ! QJFIVJ !FU ! IJ - ?J' ! ? FIZVISM?F?UTSDJTJIMT' 'JZJTSJOA ! ? I ! , DJ' M' J' FXOKJIZ' Q?
 UIJ' JK - XFU?Z ! , ' J'UTJA, . I' J' IJ' FJ' " F'OLQQUJ' QIZ' 'XTSXIX, YWQJD' FJ'ITZJTM, I ! I ! JM ? ! IQM' ! " FJ ? JI " J'
 ?AJQDUTZJ' - ? ? IQ?DITJZ ! ' M' " JF'UJLFJU' SUTTDJITJZ?JL' ? ? JFZU?FISJ' ZFIO' TZIJ ! IRSIJUZ' ? ? ? JFQ'VUJ'" "
 IJZFLFIU, 'J, Q ! IZJZQ - M' K' TJDJIU' !SQ?JMVJ ? IT' IJQQAIMTZ'LMCJ' TOZJUTJZJC? . . . J' 'FD'IXXUTAJ"
 ZFUOJTJZ?QD - AUJTJIZ ! FIITJZJQOI' TITFJWJMT - !BIID' DJ?MI' TZIJQXF - J' ? JXJJ' " TDFJ' "UVOKJZ'UJ' ! EAJUTM
 ! J' , O'LTZ ! LIJTJITFIKJ ! ' ? IB' ? ? JFQUJU' Q' S' ! ! LIX?O, F'FAJZJ' ! ! " ! IQ?DAUMTJJIST'XJO'JZK'F, JIZO' JUXII !
 QQZJ'ZIQIQJ' AUJTJIV?'X?AJ ! JZKQ' IPF' ! ! ? ZITJW?' IZQUJ ! JIXXKAIAM' JI !ZJTFUUA' JI' J, ZQQUJTJM - J'HZ?
 JTJZJ?OKDJI, JIQ?T' ?JTJV?QXIQU' IJITSF ! , XJIX'XJZITJZJIS ! DF' IIT' J, QJQJF' JVV' OQ'ZIQIKJ'XUZOL, '
 JJ - IZTZDCTJWZJTZ'CMJFIQ?ITZ' J' "UAUQTJM, JXIQOZACJZKJ, JIITFULX ! , 'JJQJADUTQJZ'JQ'JF'BFU' S' ! IJZSJZT
 ' ! SUJUM ?IAZJT'F, I' ! ! ITJ ! ? ! 'FZJQITJZJQFS' SQOF'UJQ' QIFUFJ, FISS' 'ZJJIJV' OQTJUZ ! UJNNAFF' ?SU, FJZFUJ
 "TJI - AJZJ'VOKJ' " UJ' ! MACUTJQJTM'JU?TJIQ? ' 'PZJ' ! ! LJ?JFIFLIF'J"J - ZKJ?TJ ? IT'JF'FIX'J'ITAZJ ! S' ? JZJQJQ
 ?XDJJJJWF

Permutation & Substitution Cipher: Solution



Again finding the solution is a process of small increments.

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

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

And also gives us the frequencies of
the characters →

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 '-!FeIt F?" -QU t eUF!, E7Q"D U"FO'tTtU?td L7FU. O-FeTt!!eeS -FM'
AeT-t ?tIQ "'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;!7AP '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 -leT!OFte MT"e7DQ e!OIQ "FeO'-K " XtX?K 'eT MDQ-D e'TO Ve!U?"!K L?FUt
?"FUtFFOUTA LtUTD QU T XX?UB WF-F' DQU! U FQ" Fe 'D't e?!eFUQ?LUTA tF?" E!.' MTQ? A? FeAL?U "Ut
'?t.' F"FMUA eXT eP"'Q'tA eltd "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?ISLXQO .e!l?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 tSxU." F' t'FeUTQ .FF'U SFeeS'!A. eT t Q!tU.F?" M"? T eB!
eFQeV" e!"U? .U' K eQt LAFU ee"?e"FUHB OWF?UX" F ? ,U?XeleeD 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 etLeUeK- "AF'OQ!?'e' 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.ToOVQ'
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 LQLUL" eS.?!S TXOeL !?? F'tFF'U tF eS "VF7QeU?!!t!t'
D7X" -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 eQ?"t T"FTL O' 'K- ? .D' e"IF' 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!
VeAUFULQ'VFO AU T eFTTQeQSe -tUe!t .FUL!Ut'F'U QU T A'M'! 'Qt P.ee AL'lt T"'. 't?BUeL!QQ eFV
!FU!e -? "IF?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'XtSxX.YWQ D'F 'eTt TMD.e!le M?e!eQM'!" F ? e" ?A QDUtT '-?!"IQ?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 QQeAMTt'LMC 'Tot UTet C? .. "FD'eXXUTA "tFUO Tte X?QD -AU T et!FeeT t QQe'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'DA t 'le"!!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' .tQUU T M- 'Ht? Tt t?OKDe . !OQ'T? T V?QXeQ"U" e tSFe.X
eX?X teT t teS!DF"eeT'.QQeF' VV'OQ "teQeK 'XUOL.'. -etTtDCT Wt Tt?CM FeQ ?eT "'UAUQT M.
XeQOeAC eTK . eeTFULXe." Q ADUTQ t'TQ" F7BFU'S" e StT .!SU e M?eAt T'F.e!eT ?e! 'Ft QeT t QFS'
SQOF'U Q'QeFUF .FeSS'tt eVV'OQT Ut!U NAFf'?SU.F tFU "T e-A tt!7VOK "'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?tTUQ ?St!— t' TeFl— ?F" TUQ .!UeF"QE ?F" DUtT'Ot D?UtUFL ?F— .OltTe! SeLeA'F—M
tTe— Qt?!te" .! .! tTe QST' 'XW UF tTe Ae?F tUAe L!eeFeM T?BUFL ?QSeIt?UFe" tT?t tTe— Dele L'Fe
t' TUQ .?tTel;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;K'RE ?F" DTeF tTe— !etO!Fe" M Te D?Q QO!!'OF"e" K— ?XX tTe K'—QM DT' Dele OVK! ?U"UFL ?F"
t?OFtUFL TUA DUtT TUQ BUXX?F—W TUQ 'DF .!UeF"Q t' Dele ?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'QUKXe t' "eQS!UKe tTe QSeFe DTUST F'D t' 'P VX?
Se UF tTe QST' 'XY! 'AW TeFl—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?leQqE" ?F" S'FL! ?tOX?te" K— eBel— K— UF tTe QST' 'XW AIQW 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,? Dele ?XQ' ?A'FLQt tTe .U!Qt t' KeQt'D
tTeU! ?VV! 'K?tU'F OV'F TUQ S'F"OStW Le'!Le ?F" Q' XUttXe Fe" Dele "eXULTte" Ke—'UF Ae?QO!e t' Qee
tTeU! .!UeF" 'FSe A!e A?U"e T?Vv—M ?F" T'Ve" Q' 'F t' T?Be TUA ?Q tTe STUe. UF tTeU! —'OtT.OX QV
'!tQW K?T Ut D?Q .?! "U..!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 tTe eRtleAU— . 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?IQM ?F" Q'
KKUFL ?X'O'W "IW T?!!UQM DT' T?" KeeF LUBUFL TUA ? Bel— QeBe!e XeStO!eM QtUXX Qt' .! 'Be! TUAM
UAV!eQUUFL 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 " 'IM
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
TeFl—M T'DeBeIM D?Q tTe "FX— X?" DT' "U" F't OVK! ?U" TUAE .!IM tT'OLT L!eeFe T?" KeT?Be" UF Q' "
UQL! ?Se.OX ? A?Ffe! t'D?!"Q TUAM Te S'OX" F't K?T .eeX "UQt!eQqE" t' Qee TUA ?VVe?! ?XA'Qt K!
PeFtTe?!te'W Te QtUXX !eAeAKe!e"M UF tTe AU"Qt' . TUQ H—M tT?t K?T ? .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 T?U" t'
TUAQeX.M CAOQt Ke tTe .eeXUFLQ . TUA DT' Qt?F?" S'FBUSte" . tTe S!UeAM ?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. Huliaana 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 ~ 1467

Works by:

Using multiple alphabets to encode
plain text

Switches alphabets after one or more
words



Poly-Alphabetic Cipher: Alberti cipher

Stationary disk

ABCDEFGHIJKLMNQRSTVXZ1234

Movable disk

gklnprtuz&xysomqihfdbace

Plaintext:

_LAGVERRA...

Ciphertext with index g:

AzgthpmmgQ...



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



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: 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



- ▶ 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

Theorem (Massa-energierelatie)

$$E = mc^2$$

Belangrijkste conclusie