Kryptologi

IMF, Århus Universitet

Cæsar kryptering

Jeg vil sende en besked,

MØD MIG VED HULEN KLOKKEN FIRE

Cæsar kryptering

Jeg vil sende en besked,

MØD MIG VED HULEN KLOKKEN FIRE

men for at holde beskeden hemmelig, erstatter jeg hvert bogstav med det, der står tre senere i alfabetet, og sender istedet

PBG PLJ YHG KXOHQ NORNNHQ ILUH

Cæsar kryptering

Jeg vil sende en besked,

MØD MIG VED HULEN KLOKKEN FIRE

men for at holde beskeden hemmelig, erstatter jeg hvert bogstav med det, der står tre senere i alfabetet, og sender istedet

PBG PLJ YHG KXOHQ NORNNHQ ILUH

Ø bliver til B idet vi starter forfra, hvis vi kommer til slutningen.

ABCDEFGHIJKLMNOPQRSTUVWXYZÆØÅ
DEFGHIJKLMNOPQRSTUVWXYZÆØÅABC

Er det sikkert?

Er det sikkert? Hvad hvis vi opsnapper en besked:

QVUHZ TG PRRL ÆEYL TLK P OØSLU

Er det sikkert? Hvad hvis vi opsnapper en besked:

QVUHZ TG PRRL ÆEYL TLK P OØSLU

Der er kun 28 forskellige muligheder (nøgler)

Er det sikkert? Hvad hvis vi opsnapper en besked:

QVUHZ TG PRRL ÆEYL TLK P OØSLU

Der er kun 28 forskellige muligheder (nøgler) – lad os forsøge med dem allesammen.

PUTGY SF OQQK ØDXK SKJ O NÆRKT

Er det sikkert? Hvad hvis vi opsnapper en besked:

QVUHZ TG PRRL ÆEYL TLK P OØSLU

Der er kun 28 forskellige muligheder (nøgler) – lad os forsøge med dem allesammen.

PUTGY SF OQQK ØDXK SKJ O NÆRKT
OTSFX RE NPPJ ÆCWJ RJI N MZQJS

Er det sikkert? Hvad hvis vi opsnapper en besked:

QVUHZ TG PRRL ÆEYL TLK P OØSLU

Der er kun 28 forskellige muligheder (nøgler) – lad os forsøge med dem allesammen.

PUTGY SF OQQK ØDXK SKJ O NÆRKT
OTSFX RE NPPJ ÆCWJ RJI N MZQJS
NSREW QD MOOI ZBVI QIH M LYPIR

Er det sikkert? Hvad hvis vi opsnapper en besked:

QVUHZ TG PRRL ÆEYL TLK P OØSLU

Der er kun 28 forskellige muligheder (nøgler) – lad os forsøge med dem allesammen.

PUTGY SF OQQK ØDXK SKJ O NÆRKT
OTSFX RE NPPJ ÆCWJ RJI N MZQJS
NSREW QD MOOI ZBVI QIH M LYPIR
MRQDV PC LNNH YAUH PHG L KXOHQ

Er det sikkert? Hvad hvis vi opsnapper en besked:

QVUHZ TG PRRL ÆEYL TLK P OØSLU

Der er kun 28 forskellige muligheder (nøgler) – lad os forsøge med dem allesammen.

PUTGY SF OQQK ØDXK SKJ O NÆRKT
OTSFX RE NPPJ ÆCWJ RJI N MZQJS
NSREW QD MOOI ZBVI QIH M LYPIR
MRQDV PC LNNH YAUH PHG L KXOHQ
LQPCU OB KMMG XÅTG OGF K JWNGP

Er det sikkert? Hvad hvis vi opsnapper en besked:

QVUHZ TG PRRL ÆEYL TLK P OØSLU

Der er kun 28 forskellige muligheder (nøgler) – lad os forsøge med dem allesammen.

PUTGY SF OQQK ØDXK SKJ O NÆRKT
OTSFX RE NPPJ ÆCWJ RJI N MZQJS
NSREW QD MOOI ZBVI QIH M LYPIR
MRQDV PC LNNH YAUH PHG L KXOHQ
LQPCU OB KMMG XÅTG OGF K JWNGP
KPOBT NA JLLF WØSF NFE J IVMFO

Er det sikkert? Hvad hvis vi opsnapper en besked:

QVUHZ TG PRRL ÆEYL TLK P OØSLU

Der er kun 28 forskellige muligheder (nøgler) – lad os forsøge med dem allesammen.

PUTGY SF OQQK ØDXK SKJ O NÆRKT
OTSFX RE NPPJ ÆCWJ RJI N MZQJS
NSREW QD MOOI ZBVI QIH M LYPIR
MRQDV PC LNNH YAUH PHG L KXOHQ
LQPCU OB KMMG XÅTG OGF K JWNGP
KPOBT NA JLLF WØSF NFE J IVMFO
JONAS MÅ IKKE VÆRE MED I HULEN

Er det sikkert? Hvad hvis vi opsnapper en besked:

QVUHZ TG PRRL ÆEYL TLK P OØSLU

Der er kun 28 forskellige muligheder (nøgler) – lad os forsøge med dem allesammen.

PUTGY SF OQQK ØDXK SKJ O NÆRKT
OTSFX RE NPPJ ÆCWJ RJI N MZQJS
NSREW QD MOOI ZBVI QIH M LYPIR
MRQDV PC LNNH YAUH PHG L KXOHQ
LQPCU OB KMMG XÅTG OGF K JWNGP
KPOBT NA JLLF WØSF NFE J IVMFO
JONAS MÅ IKKE VÆRE MED I HULEN

...

Kryptering ved transposition

Så vi må hellere finde på en bedre måde at kryptere vores besked.

Kryptering ved transposition

Så vi må hellere finde på en bedre måde at kryptere vores besked. Hvad hvis vi nu bare indfører en regel:

ABCDEFGHIJKLMNOPQRSTUVWXYZÆØÅ
QWERTYUIOPÅASDFGHJKLÆØZXCVBNM

Kryptering ved transposition

Så vi må hellere finde på en bedre måde at kryptere vores besked. Hvad hvis vi nu bare indfører en regel:

ABCDEFGHIJKLMNOPQRSTUVWXYZÆØÅ
QWERTYUIOPÅASDFGHJKLÆØZXCVBNM

Så fx er

MØD MIG VED HULEN KLOKKEN FIRE
SNR SOU ØTR IÆATD ÅAFÅÅTD YOJT

Kryptering ved transposition

Så vi må hellere finde på en bedre måde at kryptere vores besked. Hvad hvis vi nu bare indfører en regel:

ABCDEFGHIJKLMNOPQRSTUVWXYZÆØÅ
QWERTYUIOPÅASDFGHJKLÆØZXCVBNM

Så fx er

MØD MIG VED HULEN KLOKKEN FIRE
SNR SOU ØTR IÆATD ÅAFÅÅTD YOJT

Her er cirka $8.84 \cdot 10^{30}$ forskellige muligheder, så vi kan umuligt prøve dem allesammen.

Hvis man opsnapper en tekst, har man dog stadig god mulighed for at bryde den.

Hvis man opsnapper en tekst, har man dog stadig god mulighed for at bryde den.

QWZVSMW NGBØB VZJQFBØB KLGBRBØ ZW VBØBQ CKHLEWBØB XGSRBØ ZJMØBXBW ZN RSØEQ KØHB KM ZJVØB KJVQSJVBVB LØKMØZHHBØ QZHWSVSM BØ ZJWZGGBW ZN NKØQPM LÅ ZW NØZJZØØB VZJQFBØJBQ FKVBØ KM ABHHBGSMB KLGUQJSJMBØ RBV ADBGL ZN NZGQFB BHZSGQ KM ADBHHBQSVBØ QWBMBW HZØFZJW

Hvis man opsnapper en tekst, har man dog stadig god mulighed for at bryde den.

QWZVSMW NGBØB VZJQFBØB KLGBRBØ ZW VBØBQ CKHLEWBØB XGSRBØ ZJMØBXBW ZN RSØEQ KØHB KM ZJVØB KJVQSJVBVB LØKMØZHHBØ QZHWSVSM BØ ZJWZGGBW ZN NKØQPM LÅ ZW NØZJZØØB VZJQFBØJBQ FKVBØ KM ABHHBGSMB KLGUQJSJMBØ RBV ADBGL ZN NZGQFB BHZSGQ KM ADBHHBQSVBØ QWBMBW HZØFZJW

Vi ved, at alle bogstaver ikke optræder lige ofte i en almindelig dansk tekst.

I den opsnappede tekst ser det således ud.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
3	37	1	2	2	5	10	11	0	12	11	6	11	7

O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å
0	1	14	4	10	0	1	12	12	2	0	11	0	23	1

I den opsnappede tekst ser det således ud.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
3	37	1	2	2	5	10	11	0	12	11	6	11	7

O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å
0	1	14	4	10	0	1	12	12	2	0	11	0	23	1

Så et rimeligt gæt er, at B = E

I den opsnappede tekst ser det således ud.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
3	37	1	2	2	5	10	11	0	12	11	6	11	7

O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å
0	1	14	4	10	0	1	12	12	2	0	11	0	23	1

Så et rimeligt gæt er, at B $=$ E og Ø $=$ R.

I den opsnappede tekst ser det således ud.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
3	37	1	2	2	5	10	11	0	12	11	6	11	7

O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å
0	1	14	4	10	0	1	12	12	2	0	11	0	23	1

Så et rimeligt gæt er, at B $=$ E og Ø $=$ R. Derefter kan man gætte de andre bogstaver.

QWZVSMW NGBØB VZJQFBØB KLGBRBØ ZW VBØBQ CKHLEWBØB XGSRBØ ZJMØBXBW ZN RSØEQ KØHB KM ZJVØB KJVQSJVBVB LØKMØZHHBØ QZHWSVSM BØ ZJWZGGBW ZN NKØQPM LÅ ZW NØZJZØØB VZJQFBØJBQ FKVBØ KM ABHHBGSMB KLGUQJSJMBØ RBV ADBGL ZN NZGQFB BHZSGQ KM ADBHHBQSVBØ QWBMBW HZØFZJW

QWZVSMW NGBØB VZJQFBØB KLGBRBØ ZW VBØBQ CKHLEWBØB
XGSRBØ ZJMØBXBW ZN RSØEQ KØHB KM ZJVØB KJVQSJVBVB
LØKMØZHHBØ QZHWSVSM BØ ZJWZGGBW ZN NKØQPM LÅ ZW
NØZJZØØB VZJQFBØJBQ FKVBØ KM ABHHBGSMB KLGUQJSJMBØ
RBV ADBGL ZN NZGQFB BHZSGQ KM ADBHHBQSVBØ QWBMBW
HZØFZJW

$$\mathsf{B} = \mathsf{E} \quad \mathsf{Ø} = \mathsf{R}$$

QWZVSMW NGERE VZJQFERE KLGERER ZW VEREQ CKHLEWERE
XGSRER ZJMREXEW ZN RSREQ KRHE KM ZJVRE KJVQSJVEVE
LRKMRZHHER QZHWSVSM ER ZJWZGGEW ZN NKRQPM LÅ ZW
NRZJZRRE VZJQFERJEQ FKVER KM AEHHEGSME KLGUQJSJMER
REV ADEGL ZN NZGQFE EHZSGQ KM ADEHHEQSVER QWEMEW
HZRFZJW

QWZVSMW NGERE VZJQFERE KLGERER ZW VEREQ CKHLEWERE
XGSRER ZJMREXEW ZN RSREQ KRHE KM ZJVRE KJVQSJVEVE
LRKMRZHHER QZHWSVSM ER ZJWZGGEW ZN NKRQPM LÅ ZW
NRZJZRRE VZJQFERJEQ FKVER KM AEHHEGSME KLGUQJSJMER
REV ADEGL ZN NZGQFE EHZSGQ KM ADEHHEQSVER QWEMEW
HZRFZJW

$$G = L \quad N = F \quad V = D \quad Q = S$$

SWZDSMW FLERE DZJSFERE KLLERER ZW DERES CKHLEWERE
XLSRER ZJMREXEW ZF RSRES KRHE KM ZJDRE KJVSSJDEDE
LRKMRZHHER SZHWSDSM ER ZJWZLLEW ZF FKRSPM LÅ ZW
FRZJZRRE DZJSFERJES FKDER KM AEHHELSME KLLUSJSJMER
RED ADELL ZF FZLSFE EHZSLS KM ADEHHESSDER SWEMEW
HZRFZJW

SWZDSMW FLERE DZJSFERE KLLERER ZW DERES CKHLEWERE
XLSRER ZJMREXEW ZF RSRES KRHE KM ZJDRE KJVSSJDEDE
LRKMRZHHER SZHWSDSM ER ZJWZLLEW ZF FKRSPM LÅ ZW
FRZJZRRE DZJSFERJES FKDER KM AEHHELSME KLLUSJSJMER
RED ADELL ZF FZLSFE EHZSLS KM ADEHHESSDER SWEMEW
HZRFZJW

$$Z = A \quad W = T$$

STADSMT FLERE DAJSFERE KLLERER AT DERES CKHLEWERE
XLSRER AJMREXET AF RSRES KRHE KM AJDRE KJDSSJDEDE
LRKMRAHHER SAHTSDSM ER AJTALLET AF FKRSPM LÅ AT
FRAJARRE DAJSFERJES FKDER KM AEHHELSME KLLUSJSJMER
RED ADELL AF FALSFE EHASLS KM ADEHHESSDER STEMET
HARFAJT

STADSMT FLERE DAJSFERE KLLERER AT DERES CKHLEWERE
XLSRER AJMREXET AF RSRES KRHE KM AJDRE KJDSSJDEDE
LRKMRAHHER SAHTSDSM ER AJTALLET AF FKRSPM LÅ AT
FRAJARRE DAJSFERJES FKDER KM AEHHELSME KLLUSJSJMER
RED ADELL AF FALSFE EHASLS KM ADEHHESSDER STEMET
HARFAJT

$$F = K \quad J = N \quad K = O \quad M = G$$

STADSGT FLERE DANSKERE OLLERER AT DERES COHLEWERE XLSRER ANMREXET AF RSRES ORHE OG ANDRE ONVSSNDEDE LROGRAHHER SAHTSDSM ER ANTALLET AF FORSPG LÅ AT FRANARRE DANSKERNES KODER OG AEHHELSGE OLLUSNSNGER RED ADELL AF FALSKE EHASLS OG ADEHHESSDER STEGET HARKANT

STADSGT FLERE DANSKERE OLLERER AT DERES COHLEWERE XLSRER ANMREXET AF RSRES ORHE OG ANDRE ONVSSNDEDE LROGRAHHER SAHTSDSM ER ANTALLET AF FORSPG LÅ AT FRANARRE DANSKERNES KODER OG AEHHELSGE OLLUSNSNGER RED ADELL AF FALSKE EHASLS OG ADEHHESSDER STEGET HARKANT

$$S = I \quad L = P \quad R = V \ldots$$

STADIGT FLERE DANSKERE OPLEVER AT DERES COMPUTERE BLIVER ANGREBET AF VIRUS ORME OG ANDRE ONDSINDEDE PROGRAMMER SAMTIDIG ER ANTALLET AF FORSØG PÅ AT FRANARRE DANSKERNES KODER OG HEMMELIGE OPLYSNINGER VED HJELP AF FALSKE EMAILS OG HJEMMESIDER STEGET MARKANT

STADIGT FLERE DANSKERE OPLEVER AT DERES COMPUTERE BLIVER ANGREBET AF VIRUS ORME OG ANDRE ONDSINDEDE PROGRAMMER SAMTIDIG ER ANTALLET AF FORSØG PÅ AT FRANARRE DANSKERNES KODER OG HEMMELIGE OPLYSNINGER VED HJELP AF FALSKE EMAILS OG HJEMMESIDER STEGET MARKANT

Vi udnytter, at nogle bogstaver optræder oftere end andre.

Arthur Conan Doyle – *The Adventure of the Dancing Men*, 1898.

Arthur Conan Doyle – *The Adventure of the Dancing Men*, 1898.

I denne novelle benytter Sherlock Holmes sig af ovenstående metode til at bryde en kode, hvor hver mand svarer til et bogstav.

Viginère kryptering

Vælg et ord, fx ABE, det er vores nøgle.

Viginère kryptering

Vælg et ord, fx ABE, det er vores nøgle. Man finder så disse bogstavers placering i alfabetet.

A	1
B	2
E	5

Og rykker hvert blåt bogstav svarende til hvilket grønt der står over.

MØD MIG VED HULEN KLOKKEN FIRE

ABE ABE ABE ABEAB EABEABE ABEA

MØD MIG VED HULEN KLOKKEN FIRE

ABE ABE ABE ABEAB EABEABE ABEA

MØD MIG VED HULEN KLOKKEN FIRE

NAI NKL WGI IWQFP PMQPLGS GKWF

Hvad gør man, hvis man bliver mødt med en sådan tekst?

NJYWVÆWW ZZC XVIEQR GGAÅPDXIOIJZAG GRJNYDAG RNJ

HNT PNUVOÅ FS ÅW XDZINCPÆXXA WLRJHPNÆWW FAV IRP

SSFACIDA HUBKY

NJYWVÆWW ZZC XVIEQR GGAÅPDXIOIJZAG GRJNYDAG RNJ

HNT PNUVOÅ FS ÅW XDZINCPÆXXA WLRJHPNÆWW FAV IRP

SSFACIDA HUBKY

Husk hvordan Vigénere kryptering fungerer...

```
******** *** ****** ************** ******** ***
xxxxxxxx xxx xxxxxx xxxxxxxxxxxxxx xxxxxxxx xxx
NJYWVÆWW ZZC XVIEQR GGAÅPDXIOIJZAG GRJNYDAG RNJ

*** ******* ** ** ********** ********** *** ***
xxx xxxxxx xx xx xxxxxxxxxx xxxxxxxxxx xxx xxx
HNT PNUVOÅ FS ÅW XDZINCPÆXXA WLRJHPNÆWW FAV IRP

******** *****
xxxxxxxx xxxxx
SSFACIDA HUBKY
```

```
******** *** ****** ************** ******** ***
xxxxxxxx xxx xxxxxx xxxxxxxxxxxxxx xxxxxxxx xxx
NJYWVÆWW ZZC XVIEQR GGAÅPDXIOIJZAG GRJNYDAG RNJ

*** ****** ** ** ********** ********** *** ***
xxx xxxxxx xx xx xxxxxxxxxx xxxxxxxxxx xxx xxx
HNT PNUVOÅ FS ÅW XDZINCPÆXXA WLRJHPNÆWW FAV IRP

******** *****
xxxxxxxx xxxxx
SSFACIDA HUBKY
```

Er der nogle bogstavkombinationer, der går igen?

```
******** *** ****** ************** ******** ***
xxxxxxxx xxx xxxxxx xxxxxxxxxxxxxx xxxxxxxx xxx
NJYWVÆWW ZZC XVIEQR GGAÅPDXIOIJZAG GRJNYDAG RNJ

*** ******* ** ** ********** ********** *** ***
xxx xxxxxx xx xx xxxxxxxxxx xxxxxxxxxx xxx xxx
HNT PNUVOÅ FS ÅW XDZINCPÆXXA WLRJHPNÆWW FAV IRP

******** *****
xxxxxxxx xxxxx
SSFACIDA HUBKY
```

```
******** *** ****** ************** ******** ***
xxxxxxxx xxx xxxxxx xxxxxxxxxxxxxx xxxxxxxx xxx
NJYWVÆWW ZZC XVIEQR GGAÅPDXIOIJZAG GRJNYDAG RNJ

*** ****** ** ** ********** ********** *** ***
xxx xxxxxx xx xx xxxxxxxxxx xxxxxxxxxx xxx xxx
HNT PNUVOÅ FS ÅW XDZINCPÆXXA WLRJHPNÆWW FAV IRP

******** *****
xxxxxxxx xxxxx
SSFACIDA HUBKY
```

Så de grønne og blå bogstaver er her nok de samme...

*****ABC *** ****** **********DE ******DE ***
xxxxxXYZ xxx xxxxxx xxxxxxxxxxxxUV xxxxxxUV xxx
NJYWVÆWW ZZC XVIEQR GGAÅPDXIOIJZAG GRJNYDAG RNJ

*** ****** ** ** ********** *******ABC *** ***
xxx xxxxxx xx xx xxxxxxxxxxx xxxxxxxXYZ xxx xxx
HNT PNUVOÅ FS ÅW XDZINCPÆXXA WLRJHPNÆWW FAV IRP

******** *****
xxxxxxxx xxxxx
SSFACIDA HUBKY

```
*****ABC *** ****** ***********DE ******DE ***
xxxxxXYZ xxx xxxxxx xxxxxxxxxxxxUV xxxxxxUV xxx
NJYWVÆWW ZZC XVIEQR GGAÅPDXIOIJZAG GRJNYDAG RNJ

*** ****** ** ** ********** *******ABC *** ***
xxx xxxxxx xx xx xxxxxxxxxxx xxxxxxxXYZ xxx xxx
HNT PNUVOÅ FS ÅW XDZINCPÆXXA WLRJHPNÆWW FAV IRP

******** *****
xxxxxxxx xxxxx
SSFACIDA HUBKY
```

Afstanden mellem mønstrene er 68 og 8.

Så et godt gæt er, at nøglen består af fire bogstaver (hvorfor?).

Så et godt gæt er, at nøglen består af fire bogstaver (hvorfor?). Skriv teksten lodret, så der er 4 rækker.

NJYWVÆWW ZZC XVIEQR GGAÅPDXIOIJZAG GRJNYDAG RNJ
HNT PNUVOÅ FS ÅW XDZINCPÆXXA WLRJHPNÆWW FAV IRP
SSFACIDA HUBKY

NVZVRÅIZRDNTVSDCXRNFRFDB
JÆZIGPOAJAJPOÅZPAJÆAPAAK
YWCEGDIGNGHNÅWIÆWHWVSCHY
WWXQAXJGYRNUFXNXLPWISIU

Så et godt gæt er, at nøglen består af fire bogstaver (hvorfor?). Skriv teksten lodret, så der er 4 rækker.

```
NJYWVÆWW ZZC XVIEQR GGAÅPDXIOIJZAG GRJNYDAG RNJ
HNT PNUVOÅ FS ÅW XDZINCPÆXXA WLRJHPNÆWW FAV IRP
SSFACIDA HUBKY
```

```
NVZVRÅIZRDNTVSDCXRNFRFDB
JÆZIGPOAJAJPOÅZPAJÆAPAAK
YWCEGDIGNGHNÅWIÆWHWVSCHY
WWXQAXJGYRNUFXNXLPWISIU
```

Hver række er nu en del af teksten – hvert fjerde bogstav, og hver række er krypteret med Cæsars metode med hver sin nøgle.

Hvilke bogstaver er der flest af i hver række?

NVZVRÅIZRDNTVSDCXRNFRFDB
JÆZIGPOAJAJPOÅZPAJÆAPAAK
YWCEGDIGNGHNÅWIÆWHWVSCHY
WWXQAXJGYRNUFXNXLPWISIU

Hvilke bogstaver er der flest af i hver række?

NVZVRÅIZRDNTVSDCXRNFRFDB
JÆZIGPOAJAJPOÅZPAJÆAPAAK
YWCEGDIGNGHNÅWIÆWHWVSCHY
WWXQAXJGYRNUFXNXLPWISIU

Husk at E er det mest almindelige bogstav. Altså er det et godt gæt, at i de fire rækker svarer E til hhv. R, A, W og X.

Husk at E er det mest almindelige bogstav. Altså er det et godt gæt, at i de fire rækker svarer E til hhv. R, A, W og X. Altså at alfabetet i rækkerne er rykket hhv. 13, 25, 17 og 18 bogstaver.

Husk at E er det mest almindelige bogstav. Altså er det et godt gæt, at i de fire rækker svarer E til hhv. R, A, W og X. Altså at alfabetet i rækkerne er rykket hhv. 13, 25, 17 og 18 bogstaver. Det 13., 25. 17. og 18. bogstav i alfabetet er MYRS.

Husk at E er det mest almindelige bogstav. Altså er det et godt gæt, at i de fire rækker svarer E til hhv. R, A, W og X. Altså at alfabetet i rækkerne er rykket hhv. 13, 25, 17 og 18 bogstaver. Det 13., 25. 17. og 18. bogstav i alfabetet er MYRS.
Lad os gætte på, at nøglen er MYRE istedet...

MYREMYRE MYR EMYREM YREMYREMYREMYR EMYREMYR EMY

xxxxxxxx xxx xxxxxx xxxxxxxxxxxxxxx xxxxxxxx xxx

NJYWVÆWW ZZC XVIEQR GGAÅPDXIOIJZAG GRJNYDAG RNJ

REM YREMYR EM YR EMYREMYREMY REMYREMYRE MYR EMY

xxx xxxxxx xx xx xxxxxxxxxxx xxxxxxxxxx xxx xxx

HNT PNUVOÅ FS ÅW XDZINCPÆXXA WLRJHPNÆWW FAV IRP

REMYREMY REMYR

xxxxxxxx xxxxx

SSFACIDA HUBKY

MYREMYRE MYR EMYREM YREMYREMYREMYR EMYREMYR EMY
ANGRIBER MAN SIMPLE KRYPTOSYSTEMER BENYTTER MAN
NJYWVÆWW ZZC XVIEQR GGAÅPDXIOIJZAG GRJNYDAG RNJ

REM YREMYR EM YR EMYREMYREMY REMYREMYRE MYR EMY
SIG TYPISK AF DE STATISTISKE EGENSKABER VED DET
HNT PNUVOÅ FS ÅW XDZINCPÆXXA WLRJHPNÆWW FAV IRP

REMYREMY REMYR
ANVENDTE SPROG
SSFACIDA HUBKY

Kan intet af det du fortælle os bruges til noget som helst?

- Hvis nøglen i Vigènere er lang nok, eller man benytter flere nøgler efter hinanden, er det en ret sikker kode.

Kan intet af det du fortælle os bruges til noget som helst?

- Hvis nøglen i Vigènere er lang nok, eller man benytter flere nøgler efter hinanden, er det en ret sikker kode.
- Koder af denne type blev bruget under 2. verdenskrig.

Kan intet af det du fortælle os bruges til noget som helst?

- Hvis nøglen i Vigènere er lang nok, eller man benytter flere nøgler efter hinanden, er det en ret sikker kode.
- Koder af denne type blev bruget under 2. verdenskrig.

- Her var længden af nøglen længere end beskederne, så metoden ovenfor kunne ikke bruges til at bryde den.

- Hvis man komprimerer ('zipper') sin tekst før man krypterer er det meget mere sikkert, idet komprimering minimerer de mønstre, der naturligt er i sproget, og som vi udnyttede flere gange, da vi brød krypteringen.

- Hvis man komprimerer ('zipper') sin tekst før man krypterer er det meget mere sikkert, idet komprimering minimerer de mønstre, der naturligt er i sproget, og som vi udnyttede flere gange, da vi brød krypteringen.
- Dankortet benytter kryptering ved transposition, men med et meget stort 'alfabet' ($2^{64} \approx 1,8 \cdot 10^{19}$).

Hvad med netbank?

- Det er upraktisk og usikkert, hvis banken skal gemme nøgler for hver kunde.

Hvad med netbank?

- Det er upraktisk og usikkert, hvis banken skal gemme nøgler for hver kunde.
- Der findes en krypteringsmetode, hvor man ikke kan låse en besked op med samme nøgle, som den kan låses med – RSA.

Hvad med netbank?

- Det er upraktisk og usikkert, hvis banken skal gemme nøgler for hver kunde.
- Der findes en krypteringsmetode, hvor man ikke kan låse en besked op med samme nøgle, som den kan låses med – RSA.
- Dermed kan banken have en offentlig nøgle, som alle kan kryptere beskeder med, men kun banken kan læse beskederne igen.