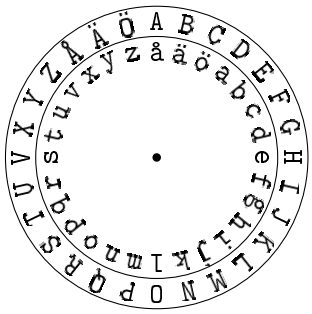
Caesarchiffer

Nedanstående uppgifter löses lämpligast med hjälp av en kryptosnurra:



I figuren ovan är snurran inställd med en förskjutning av alfabetet med 3 steg. Med denna inställning av snurran ska t ex `a` krypteras som `D` och `r` ska krypteras som `U`.

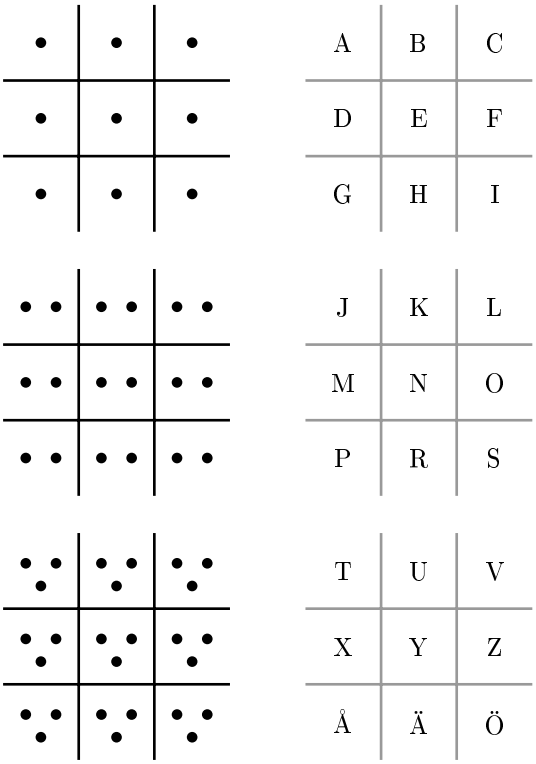
1. Meddelandet `GHFHPEHU` har krypterats med en förskjutning av 3 steg. Hur lyder klartexten?

2. Det krypterade meddelandet `FAOÄKÅGP` har erhållits genom kryptering med en förskjutning mellan 11 och 17. Bestäm klartexten.

3. Kryptogrammet `BÄGFCAN` har krypterats med okänd förskjutning. Hur lyder klartexten?

Murarchiffer

Vid kryptering ersätter man varje bokstav enligt nedanstående schema, t ex krypteras A som ⬝⌟, M som ⚃ och Z som ⚅.



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

1. Kryptera KARLSKRONA.

2. Dekryptera ⌞⚀⌟ ⌝⌟⚃⚀⚁.

3. Man kan kastat om ordningen på de vänstra rutnäten och sedan krypterat ett meddelande. Vad döljer sig bakom

⌞⚀⚁⌟⚃⚀?

4. I denna uppgift skriver vi, innan kryptering, bokstäverna ABCDEFGHI, JKLMNOPRS respektive TUVXYZÅÄÖ i varsin kolumn i de högra rutnäten ovan (fast nödvändigtvis inte i nämnd ordning). Rutnäten har kvar sina ursprungliga platser enligt ovan. Knäck meddelandet

⚀⌞⌞⌞⌞⚃⌞ ⚂⚀⌞⚁⚂⌞ .

Playfair

Grupperar klartexten i block om två bokstäver vardera. Om bokstäverna i ett block skulle vara lika skjuter man in ett `x` mellan dessa och grupperar om klartexten. Eventuellt behöver man lägga man till ett `x` i slutet för att sista blocket för att göra den till ett bigram. Bokstaven `j` ersätts med ett `ii`. Ett första försök att gruppera klartexten

`as slippery as an eel`

ger resultatet

`as sl ip pe ry as an ee l`,

vilket måste justeras eftersom nästsista blocket är en dubbelbokstav och sista blocket består av endast en bokstav. Efter att lagt till ett `x` mellan de två `e`:na erhållerna hon

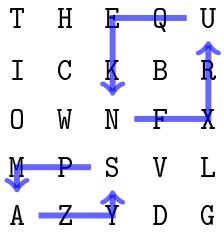
`as sl ip pe ry as an ex el`.

Krypteringsnyckeln ges av en tabell om fem rader och fem kolumner, som t ex följande tabell. se den

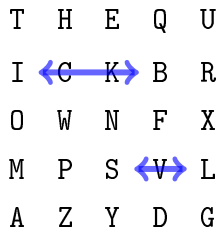
T	H	E	Q	U
I	C	K	B	R
O	W	N	F	X
M	P	S	V	L
A	Z	Y	D	G

Med hjälp av tabellen krypteras varje block enligt följande tre regler.

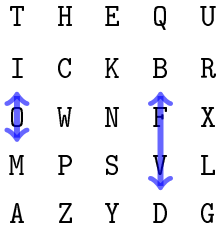
1. Om bokstäverna i ett block förekommer på olika rader och kolumner, så ersätts de med den bokstav på samma rad som respektive bokstav och på samma kolumn som den andra bokstaven i blocket. Vi har t ex att `as` krypteras som `YM`, `sa` som `MY`, `un` som `EX` och `nu` som `XE`.



2. Om bokstäverna i ett block förekommer i samma rad, ersätts respektive bokstav av den direkt till höger i tabellen, t ex krypteras `ib` som `CR` och `bi` som `RC`. Om en av bokstäverna står i femte kolumnen, ersätts den med bokstaven i första kolumnen på samma rad, t ex ersätts `sl` med `VM` och `ls` med `MV`.



3. Om bokstäverna i ett block förekommer i samma kolumn, ersätts respektive bokstav av den direkt under i tabellen, t ex ersätts `im` med `OA` och `mi` med `AO`. Om en av bokstäverna förekommer i femte raden ersätts den av bokstaven på första raden på samma kolumn, t ex krypteras `bd` som `FQ` och `db` som `QF`.



Klartexten `as slippery as an eel` ger oss kryptogrammet

`YM VM CM SH KG YM YO UN US`.

Givetvis tar man bort ordmellanrummen innan man sänder kryptogrammet.

1. Kryptogrammet

`IXMZRSGI`

har erhållits med samma nyckel som i exemplet ovan. Bestäm klartexten.

2. Vi har lyckats kncäka delar av nyckeln till ett Playfair-krypto:

```
M       X
  L   U
    Z
  H   O
B       T
```

Vidare vet vi också att

`bo` krypteras som `KF`
`ep` krypteras som `YD`
`gi` krypteras som `ZB`
`ht` krypteras som `QV`
`iz` krypteras som `RN`
`lm` krypteras som `CE`
`lu` krypteras som `AS`.

Fyll i resten av tabellen.

3. När meddelandet

`vad blir nio plus elva`

krypteras med Playfair får man kryptogrammet

`KVAGTROCOHQZVHCUKV.`

Tidigare har Eve lyckats knäcka delar av nyckeln och då funnit följande tabell.

O				I
				X
Y			F	
		V		
			C	W

Knäck nyckeln och dekryptera sedan kryptogrammet

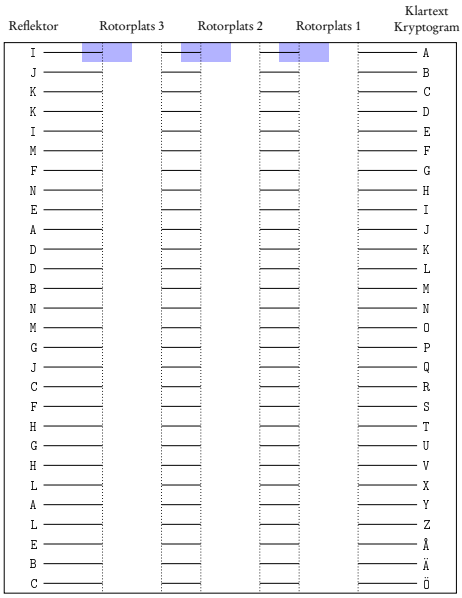
`UESBMSWZKCVBVMOBHTWXSFUGVH.`

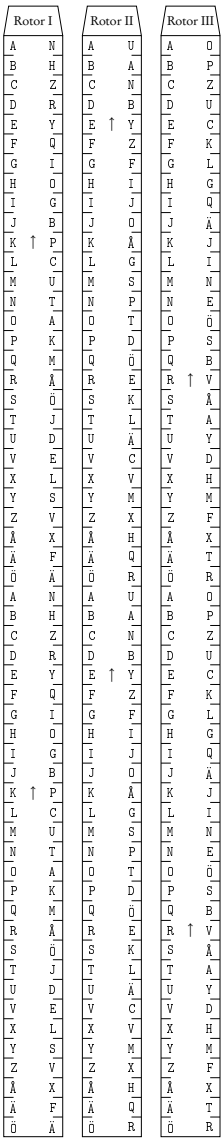
Swedish Paper Enigma machine (SPE)

1. Kryptera ditt namn och dekryptera sedan resultatet.

SPE: Swedish Paper Enigma machine

Inspirerad av den engelska versionen utvecklad av Michael C. Koss.





Val av nyckel

Väl en permutation (r_1, r_2, r_3) av rotor I, II och III $(a_1, a_2, a_3) \in \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Ö}\}$.

Innan kryptering och dekryptering

Placera rotor r_k i rotorplats k. Ställ varje rotor i sin startposition, d v s skjut respektive rotor så att bokstaven a_k hamnar vid den blå rektangeln.

Kryptering och dekryptering

Antag att vi ska kryptera eller dekryptera $x \in \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Ö}\}$.

1. Skjut rotor r_1 en rad upp. Om rotor r_1 eller r_2 har en pil (↑) längst upp och som då försvinner ska även rotorn till vänster skjutas en rad upp.
2. Leta upp x i kolumnen *Klartext/Kryptogram* och följ linjen från x till bokstaven y i den högra kolumnen i rotor r_1.
3. Leta upp y i den vänstra kolumnen i rotor r_1. Följ linjen från y till rotor r_2 och upprepa proceduren för rotor r_2 och r_3..
4. Låt z vara bokstaven vi når i kolumnen *Reflektor* efter att också passerat rotor r_3. Leta den andra kopian z i kolumnen och följ linjen från denna till rotor r_3.
5. Upprepa proceduren i steg 2, fast i omvänd ordning, d v s avläs vänstra kolumnen i rotorn och leta upp motsvarande bokstav i högra kolumnen.
6. Upprepa steg 5 för rotor r_2 och sedan r_1.
7. Slutligen når man X i kolumnen *Klartext/Kryptogram* vilken är det x ska ersättas med.
8. Gå tillbaka till steg 1 om fler bokstäver ska krypteras eller dekrypteras.