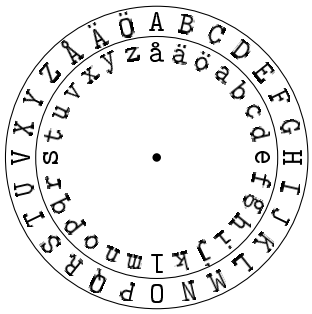
Caesarchiffer

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?

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

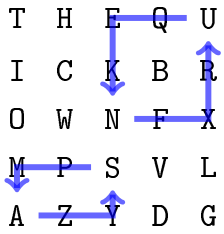
`as sl ip pe ry as an ex el`.

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

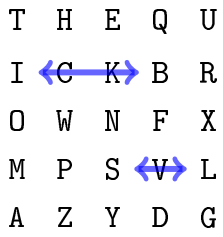
T	H	E	Q	U
I	C	K	B	R
O	W	N	F	X
M	P	S	V	L
A	Z	Y	D	G

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

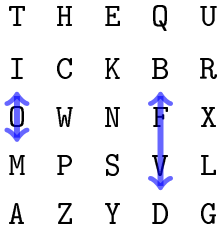
1. Om bokstäverna i ett block förekommer på olika rader och kolumner, så ersätts de med den bokstav på samma rad som respektive bokstav och på samma kolumn som den andra bokstaven i blocket. Vi har t ex att `as` krypteras som `YM`, `sa` som `MY`, `un` som `EX` och `nu` som `XE`.



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.`