

Enigma

Enigma var en maskin som ble brukt av tyskerne under 2. verdenskrig til å kryptere (dvs. skule innholdet i) meldinger. Den kom i flere varianter, men den enkleste bestod av tre scramblerhjul, og det er den vi skal se på.

Hvert scramblerhjul hadde 26 kontakter på hver side. Kontaktene på høyre side av det første hjulet representerte bokstavene A-Z. Hver kontakt var forbundet med nøyaktig en kontakt på den andre siden av hjulet. Scramblerhjulene stod i kontakt med hverandre, slik at et inputsignal fra en posisjon på høyre side av det første hjulet ble konvertert til en ny posisjon på venstre side av det første hjulet, som så ble først videre til samme posisjon på høyre side av det neste hjulet osv.

På enden av rekken med scramblerhjul var det plassert en “reflektor”, som tok et signal på en posisjon på høyre side og overførte dette til en ny posisjon på samme side. Reflektoren var symmetrisk, dvs. at dersom den tok bokstav A og gjorde den om til bokstav B, så ville også B bli til A.

Så fortsatte signalet tilbake gjennom scramblerhjulene i motsatt rekkefølge, før de endte opp på en viss posisjon på høyre side av det første hjulet igjen. Denne posisjonen representerte en bokstav, som lyste opp på et lampebrett og så skrev man ned bokstaven som lyste opp.

For hver bokstav man skrev, roterte det første hjulet en plass, og når det var gått en hel gang rundt, roterte det andre hjulet en plass, dvs. at etter den 26. bokstaven har blitt skrevet inn, så vil det første hjulet rotere tilbake til startposisjonen og det andre hjulet rotere en plass. Når det andre hjulet var gått en hel gang rundt roterte det tredje hjulet en plass. Reflektoren endret aldri posisjon.

Vi trenger din hjelp til å kryptere noen meldinger med en slik Enigma, men dessverre har vår mekaniske versjon tatt kvelden, så vi trenger en digital versjon i steden.

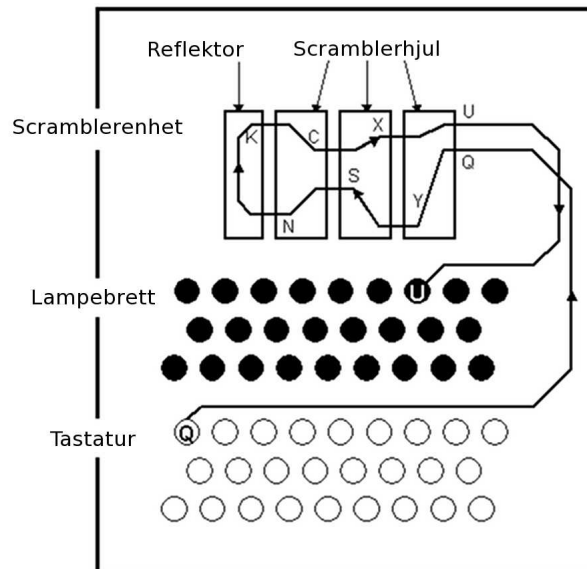


Figure 1: Skjematisk oversikt over Enigma-maskin

Input

Først et heltall N , lengden på meldingen som skal krypteres. Deretter følger en linje med N store, engelske bokstaver (A-Z).

Så følger tre linjer, hver med 26 store, engelske bokstaver, som representerer startposisjonen og koblingene til hvert av scramblerhjulene (fra høyre til venstre). Hvis bokstaven på plass nummer i er W , betyr det at hjulet konverterer signalet på denne plassen til bokstaven W (plass nummer 22). Når hjulet roterer, tilsvarer dette at man flytter den første bokstaven bakerst og flytter alle andre fremover en plass.

Til sist følger koblingene i reflektoren, også som 26 store, engelske bokstaver, oppgitt på samme måte som for scramblerhjulene.

Output

En linje med den krypterte meldingen.

Begrensninger

$$1 \leq N \leq 20,000$$

Eksempel 1

Input	Output
6 ATTACK EKMFLGDQVZNTOWYHXUSPAIBRCJ AJDKSIRUXBLHWTMCQGZNPYFVOE BDFHJLCPRTXVZNYEIWGAKMUSQO YRUHQSLDPXNGOKMIEBFZCWVJAT	NCRRFG

Kommentarer

Det kan være lurt å sette opp alfabetet over beskrivelsen av hvert hjul. For den første bokstaven A følger vi hjulene mot venstre og tilbake igjen slik:

1. hjul
ABCDEFGHIJKLMNOPQRSTUVWXYZ
|
EKMFLGDQVZNTOWYHXUSPAIBRCJ

2. hjul
ABCDEFGHIJKLMNOPQRSTUVWXYZ
|
AJDKSIRUXBLHWTMCQGZNPYFVOE

3. hjul
ABCDEFGHIJKLMNOPQRSTUVWXYZ
|
BDFHJLCPRTXVZNYEIWGAKMUSQO

Reflektor
ABCDEFGHIJKLMNOPQRSTUVWXYZ
|
YRUHQSLDPXNGOKMIEBFZCWVJAT

3. hjul
BDFHJLCPRTXVZNYEIWGAKMUSQO
|
ABCDEFGHIJKLMNOPQRSTUVWXYZ

2. hjul

AJDKSIRUXBLHWTMCQGZNPYFVOE
|
ABCDEFGHIJKLMNOPQRSTUVWXYZ

1. hjul

EKMFLGDQVZNTOWYHXUSPAIBRCJ
|
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Når det første hjulet roteres blir den nye konfigurasjonen slik, og vi kan følge den neste bokstaven (T) frem og tilbake:

1. hjul

ABCDEFGHIJKLMNOPQRSTUVWXYZ
|
KMFLGDQVZNTOWYHXUSPAIBRCJE

2. hjul

ABCDEFGHIJKLMNOPQRSTUVWXYZ
|
AJDKSIRUXBLHWTMCQGZNPYFVOE

3. hjul

ABCDEFGHIJKLMNOPQRSTUVWXYZ
|
BDFHJLCPRTXVZNYEIWGAKMUSQO

Reflektor

ABCDEFGHIJKLMNOPQRSTUVWXYZ
|
YRUHQSLDPXNGOKMIEBFZCWVJAT

3. hjul

BDFHJLCPRTXVZNYEIWGAKMUSQO
|
ABCDEFGHIJKLMNOPQRSTUVWXYZ

2. hjul

AJDKSIRUXBLHWTMCQGZNPYFVOE
|
ABCDEFGHIJKLMNOPQRSTUVWXYZ

1. hjul
KMFLGDQVZNTOWYHXUSPAIBRCJE
|
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Tilsvarende kan vi rotere første hjulet og følge de neste fire bokstavene gjennom hjulene for å få svaret *NCRRFG*.

Eksempel 2

Input
77 NLANHKGWKZVMYQNAHTOLEXCAIDXVEIBHXBPNWWVWBLXJBWJVMRYAMPOPDJHJASNMIWHYJPYGKJT GDQVZNTOWYHXUSPAIBRCJEKMFL CQGZNPYFVOEAJDKSIRUXBLHWTM QOBDHFHJLCPRTXVZNYEIWGAKMUS YRUHQSLDPXNGOKMIEBFZCWVJAT
Output
IFYOUCANREADTHISYOUAREPROBABLYALMOSTDNEWITHTASKNUMBERONEOFNIOCONGRATULATIONS

Kommentarer

I dette eksempelet vil også det 2. hjulet begynne å rotere.