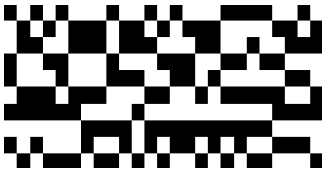
Grafisk kryptografi
(hemmelig koding av bilder)

Legg den løse platen nøyaktig over den faste og se hva som skjer.

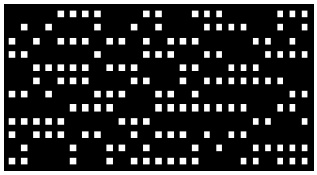
Hvordan kan det brukes?

Grete skal til Australia, og mens hun er der kan hun få behov for å sende en hemmelig melding til Hans.

1 Før hun drar lager de *nøkkelen* for den hemmelige koden. Nøkkelen er laget ved hjelp av et helt tilfeldig mønster. Grete tar med seg et eksemplar til Australia og Hans beholder ett eksemplar i Norge. Nøkkelen må de holde hemmelig.



2 I Australia lager Grete en *kryptert melding* ved hjelp av *nøkkelen* og beskjeden hun vil kode, for eksempel *Jeg elsker deg*.

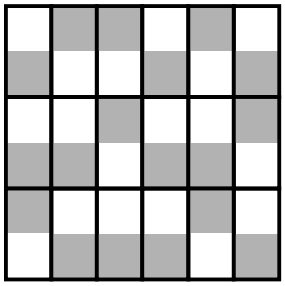


3 Grete sender den krypterte meldingen i et brev til Hans uten å være redd for at noen som skal få tak i brevet klarer å dekode det.

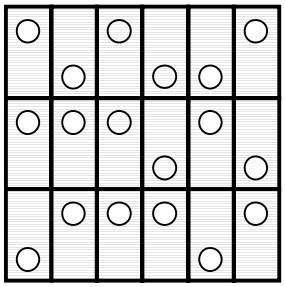
4 Når Hans får brevet legger han den krypterte meldingen over nøkkelen, og bare da kan han lese meldingen.

Hvordan virker dette?

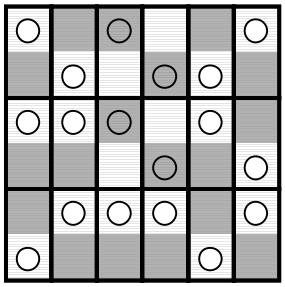
1 ***Nøkkelen*** består av grupper på to og to ruter. I hver gruppe er det en hvit og en sort rute. Hvilken av de to rutene som er hvit og hvilken som skal være sort velges helt tilfeldig, for eksempel ved å kaste terning.



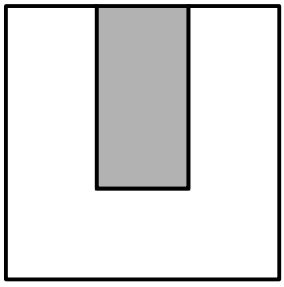
2 ***Den kodede meldingen*** er bygget opp på samme måten. Den er sort over det hele, med ett *"hull"* i hver gruppe på to ruter.



3 Når vi legger arkene over hverandre, ser vi hvordan dette virker. Hullene er plassert over et hvitt felt der vi ønsker et lyst resultat, og over et sort felt der vi ønsker et mørkt resultat.



4 Her ser du hvilken "melding" vi har kodet i dette eksempelet.



Når *nøkkelen* består av et helt tilfeldig mønster, vil også *den kodede meldingen* bestå av et tilfeldig mønster, og denne koden vil da være *helt umulig å knekke*. Kun de som har tilgang på både nøkkel og kodet melding sammen vil kunne dekode den.

Litt mer om kryptering

Akkurat denne krypteringsmetoden vi har sett på her brukes nok ikke i praksis, men den illustrerer et generelt prinsipp:

- Ved krypteringen brukes en *nøkkel* og en *krypteringsmetode* for å kode meldingen.
- Ved dekryptering brukes en *nøkkel* og en *dekrypteringsmetode*.

I dette tilfellet er begge nøklene like og må holdes hemmelige, men metoden som brukes behøver ikke å være hemmelig.

Det finnes også krypteringsmetoder der nøklene ikke er like. Et spesielt eksempel er "*offentlig nøkkel kryptering*" (public key cryptography). Med den teknikken kan hvem som helst kryptere meldinger ved hjelp av en nøkkel som er åpent tilgjengelig. Bare de som har den hemmelige dekrypteringsnøkkelen kan dekode meldingene.

Eksempel: Du kan bruke bankens *offentlige nøkkel* (som alle kjenner) til å kryptere en meldingen før du sender den til banken. Kun banken som har den *private nøkkelen* klarer å dekode meldingen din.

Uten at du merker det er teknikker som dette inne i bildet når du bruker banktjenester over Internet eller besøker såkalte *sikre web-sider*.

Vil du lage dine egne kodede bilder?

Det går bra med to papirark også hvis du holder dem opp mot et vindu. På **http://members.xoom.com/helger** finner du denne beskrivelsen og et PC-program som du kan bruke til å kode dine egne bilder.

Her trengs tre ark for å lese koden

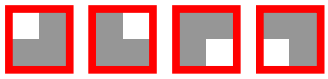
Løft opp plastflakene og kontroller selv

Her ligger en prøve på denne kodingen

1. Ark 1 er fylt opp av ruter som vist til høyre, tilfeldig fordelt.

1. Ark 2 er fylt opp av ruter som vist til høyre, tilfeldig fordelt.

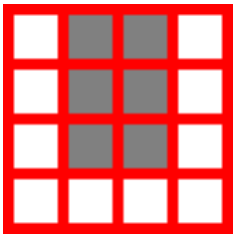
2. Når en rute fra ark 1 legges oppå en rute fra ark 2, blir resultatet et av alternativene til høyre.



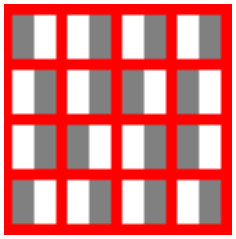
3. Ark 3 er fylt opp av ruter som vist til høyre. For hver rute velges den varianten som gir korrekt resultat (helt sort eller ett hvitt hjørne) når alle arkene ligger over hverandre.

Eksempel:

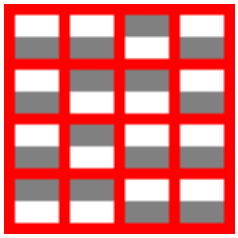
Bildet vi vil kode



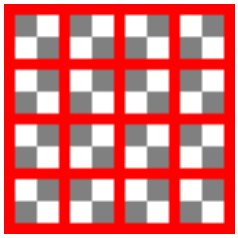
Ark 1



Ark 2



Ark 3

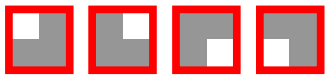


Ark 1, 2 og 3 over hverandre

Her trengs bare to av tre ark for å lese koden

Her ligger en prøve på denne kodingen

1. Ark 1 er fylt opp av ruter som vist til høyre, tilfeldig fordelt.



2. Ark 2 er fylt opp av ruter med de samme mønstre etter følgende regler:
   - I de ruter vi ønsker hvitt resultat velges samme mønster som i ark 1.

   - I de ruter vi ønsker sort resultat brukes speilbildet av ruten i ark 1 om en horisontal akse.

3. Ark 3 er fylt opp på samme måte som ark 2, men rutene er speilet om en vertikal akse.

Eksempel: