

ANELU AT YR
ANHYSGOEL

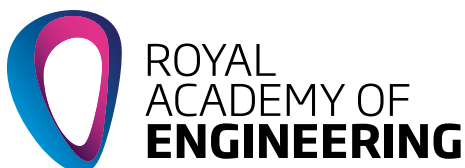
2018

1918



Torri codau

Canllaw'r
Myfyriwr



ROYAL
ACADEMY OF
ENGINEERING



Nod yr adnodd hwn yw rhoi cyfle i fyfyrwyr ymchwilio i effaith gwyddoniaeth, technoleg, peirianeg a mathemateg (STEM) ar dorri codau a diogelwch.

Ysbio

Yn dilyn yr Ail Ryfel Byd, cynyddu wnaeth tensiynau rhwng y Bloc Dwyreiniol (yr Undeb Sofietaidd a'i gwladwriaethau lloeren) a'r Bloc Gorllewinol (UDA a'u chynghreiriaid NATO).

Cyfeiriwyd at y cyfnod hwn fel y 'Rhyfel Oer' oherwydd na chafwyd unrhyw ymladd rhwng y ddwy ochr. Dechreuodd y Rhyfel Oer ar ôl yr Ail Ryfel Byd, gan barhau tan y 1990au. Ond roedd ar ei hanterth yn y 1960au.

Roedd cyfrinachedd ac ysbio yn rhan fawr o'r tyndra yn Ewrop yn ystod y cyfnod hwn. Mae tair prif nodwedd i'r gweithrediadau ysbio a ddiwyddodd yn ystod y Rhyfel Oer:

- » Ysbiwyr yn casglu dogfennau a thystiolaeth.
- » Gwrthysbio.
- » Gweithrediadau cudd.

Mewn ffilmiau ac ar y teledu, mae ysbiwyr yn cael eu portreadu fel unigolyn sy'n cael pob math o anturiaethau cyffrous. Mewn gwirionedd, mae ysbiwyr yn bobl sy'n byw bywydau digon cyffredin, heb sefyll allan o gwbl. Dydyn nhw ddim eisiau tynnu sylw at yr hyn maen nhw'n ei wneud, yn enwedig gan eu bod fel arfer yn gweithio ar waith cyfrinachol neu fod ganddynt gysylltiadau cyfrinachol iawn.

AMSER I WNEUD

Mae sawl ffordd o godio, neu amgryptio, neges i'w chadw'n gyfrinachol oddi wrth eich gelynion.

Un ffordd o amgryptio'ch neges yw defnyddio seiffr amnewid, sy'n amnewid un llythyren gydag un arall. Mae sawl ffordd o ddefnyddio'r seiffr hwn ond y ffordd hawsaf yw amnewid gyda'r llythyren nesaf yn y wyddor. Caesar Shift 2 yw enw hyn. Er enghraifft, mae 'a' yn troi'n 'b', mae 'b' yn troi'n 'c' ac yn y blaen.

Pe baech chi am amgryptio'r gair 'peirianeg' gan ddefnyddio'r seiffr hwn, byddai'n troi'n 'qdsjbooffh'.

- » Rhowch gynnig ar amgryptio'ch enw gyda'r seiffr hwn.
- » Beth fyddai'ch enw pe baech chi'n amgryptio gan ddefnyddio Caesar Shift 2, lle mae pob llythyren yn cael ei hamnewid gyda'r llythyren sydd ddau safle o'i blaen yn y wyddor?

Mae dehongli pob llythyren yn unigol yn llafurus iawn. I gyflymu'r broses fe allech chi amgryptio'r wyddor yn gyntaf.

I wneud peiriant i amgryptio'r wyddor, byddwch angen:

- » Cerdyn neu gardbord
- » Pin hollt
- » Taflen gymorth yn torri codau

Dull

1. Gludwch y daflen gymorth ar gerdyn neu gardbord ac yna torrwyd allan yr olwynion cod.
2. Gosodwch yr olwyn fach y tu mewn i'r olwyn fawr, a'i dal yn ei lle gyda'r pin hollt.
3. Nawr gallwch chi droi'r olwyn fewnol fel ei bod yn cyd-fynd â llythyren wahanol ar yr olwyn allanol.
4. Ysgrifennwch neges i'w hanfon at ffrind.
5. Dewch o hyd i'r llythrennau ar yr olwyn fewnol. Defnyddiwch ei chymar ar yr olwyn allanol i'w hysgrifennu mewn cod.

Defnyddiwch Caesar Shift 14 i anfon eich neges mewn cod at eich ffrind. Allwch chi ddadgodio'r neges anfonon nhw atoch chi?

I ddadgodio'r neges, rhaid i chi ddod o hyd i bob llythyren ar yr olwyn allanol ac ysgrifennu ei chymar ar yr olwyn fewnol.

YMESTYN A HERIO

Er mwyn sicrhau bod negeseuon yn cael eu trosglwyddo'n hwylus, byddai'r un cod yn cael ei ddefnyddio ar gyfer pob neges mewn un diwrnod.

Byddai'r cod yn newid bob dydd am hanner nos i atal y gelyn rhag datglo'r cod a dadgodio'r negeseuon i gyd.

Rydych chi wedi rhyng-gipio neges sy'n dweud:

D NZIO TJP V AJJY KVXFVBZ WT XVM

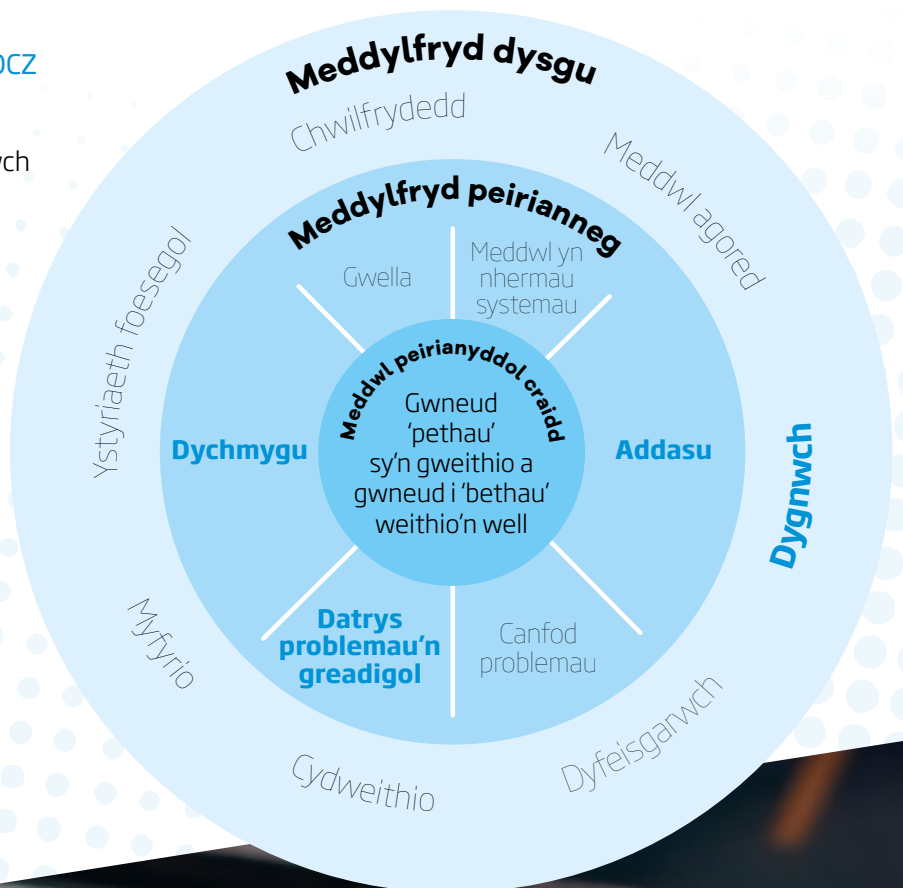
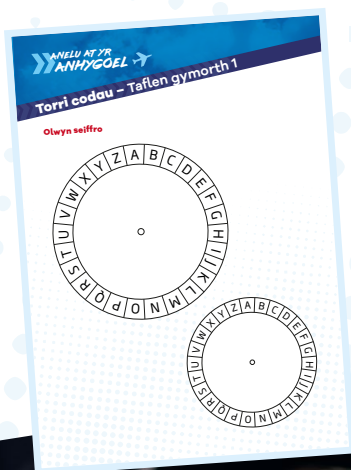
Ceisiwch ddehongli beth mae'r neges yn ei ddweud ac felly'r cod amgryptio.

Nawr eich bod chi'n gwybod y cod amgryptio ar gyfer heddiw, gallwch chi ddadgodio holl negeseuon y diwrnod. Beth mae'r negeseuon hyn yn ei ddweud?

- [OCZ XVM RDGG YZGDQZM OCZ KVXFVBZ OJ NXCJJG](#)
- [OCZ AJJY KVXFVBZ XJOVDIN V HVK](#)
- [OCZ HVK RDGG NCJR OCZ GJCVDJJI JA OCZ NZXMZO GVVJMVOJMT](#)

Gyda'r cod amgryptio ar gyfer heddiw, gallwch chi anfon negeseuon ffug i ddrysu ysbiwyr y gelyn. Codiwch neges gyda'r cod ar gyfer heddiw a'i hanfon at ffrind i wneud iddo feddwl fod y lleoliad dosbarthu wedi newid.

Gall dehongli pob neges, un llythyren ar y tro, fod yn llafurus iawn. Defnyddiwch Excel i greu datgodiwr awtomatig.





ROYAL ACADEMY OF ENGINEERING

Academi Frenhinol Peirianeg

Fel academi genedlaethol y DU ar gyfer peirianeg, rydym ni'n dwyn ynghyd y peirianwyr mwyaf llwyddiannus a dawnus gydag un nod: hybu a hyrwyddo rhagoriaeth ym maes peirianeg.

Mae gennym ni bedair her strategol:

Sicrhau bod y DU ar flaen y gad ym maes arloesedd peirianyddol

Cefnogi datblygiad arloesedd a busnesau peirianyddol llwyddiannus yn y DU er mwyn creu cyfoeth, swyddi a buddiannau i'r genedl.

Mynd i'r afael â'r argyfwng o ran sgiliau peirianeg

Diwallu anghenion y DU drwy ysbrydoli cenhedlaeth o bobl ifanc o bob cefndir a rhoi iddynt y sgiliau ansawdd uchel sydd eu hangen arnynt i gael gyrfa werth chweil ym maes peirianeg.

Rhoi lle canolog i beirianeg mewn cymdeithas

Gwella ymwybyddiaeth a chydabyddiaeth y cyhoedd o rôl hollbwysig peirianwyr ym mhob man.

Arwain y proffesiwn

Manteisio ar arbenigedd, egni a gallu'r proffesiwn i osod cyfeiriad strategol ar gyfer peirianeg a chydweithio ar atebion i brif heriau peirianeg.



Nod y Rhaglen Ieuentid a STEM RAF 100 yw cynnwys ac ysbrydoli pobl ifanc drwy feithrin eu diddordeb mewn llwybrau gyrfa peirianyddol a thechnegol.

O arbenigwyr seiber i awyrofod, awyrennau, electroneg a disgyblaethau mecanyddol, mae'r RAF wedi ymrwmo i ddefnyddio dathliadau ein canmlwyddiant i roi cyfle i bawb ac i annog mwy o amrywiaeth yn y maes hollbwysig hwn o brinder sgiliau cenedlaethol.



Academi Frenhinol Peirianeg
Prince Philip House, 3 Carlton House Terrace, Llundain SW1Y 5DG

Ffôn: +44 (0)20 7766 0600
www.raeng.org.uk

Rhif elusen gofrestredig 293074

Delwedd clawr blaen: Shutterstock.com
Delwedd clawr cefn: Shutterstock.com

Ailgylchwhch yr adnodd hwn (mae'r clawr wedi'i drin â laminiad y gellir ei ailgylchu)