GWEITHGAREDD STEM 3
NODIADAU'R ATHRO

CYFATHREBU

raf100schools.org.uk

Y CYFARPAR SYDD EI ANGEN AR GYFER POB PÂR O FYFYRWYR:

- Cyflenwad pŵer e.e. 2xD cell
- Pedair gwifren gysylltu
- Dwy wifren gysylltu hir (mae modd uno nifer o wifrau byrrach i wneud gwifrau hirach)
- Dau fylb a dalwyr
- Switsh
- Pin hollti (neu bin bawd a chorcyn)
- Dau gopi o'r Templed Dryswr
- Papur ysgrifennu
- Dau gopi o'r daflen gwaith estynedig STEM (dewisol)

CYSYLLTIADAU Â'R CWRICWLWM FFISEG: CYLCHEDAU CYFOCHROG A CHYFRESOL; SIGNALAU DIGIDOL

GWEITHGAREDD STEM: CYLCHEDAU CYFATHREBU

Yn y gweithgaredd hwn mae myfyrwyr yn dylunio cylched drydan ac yn ymchwilio i sut mae'n gallu cael ei defnyddio i anfon negeseuon wedi'u hamgodio a'u hamgryptio.

Cyflwynwch y gweithgaredd drwy chwarae'r fideo cysylltiedig: *Codebreakers*. Eglurwch yn ystod yr Ail Ryfel Byd i'r ddwy ochr osod cannoedd o filltiroedd o geblau trydanol er mwyn cyfathrebu ar y tir. Roedd modd anfon negeseuon yn gyflym rhwng yr anfonwr a'r derbynnydd drwy ddefnyddio switsh i dapio'r neges mewn cod Morse (smotiau a dashiau) a defnyddio dryswyr i gymysgu'r llythrennau cyn anfon y neges fel mai dim ond rhywun arall a oedd yn gwybod gosodiadau'r dryswr allai ddadgryptio'r neges.

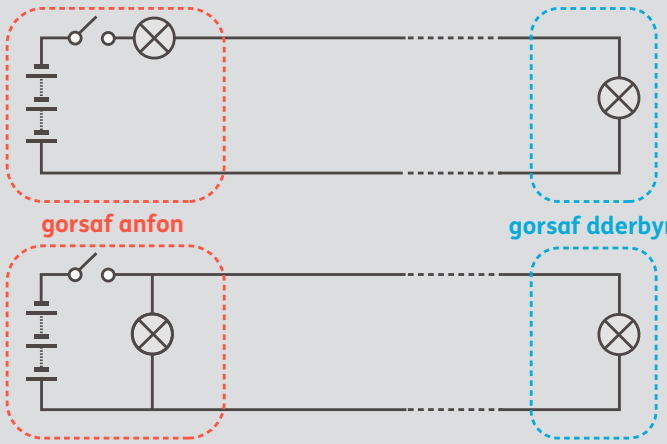
Dylai myfyrwyr ddilyn y cyfarwyddiadau ar gyfer y gweithgaredd STEM i ddylunio dolen gyfathrebu un ffordd (telegraff trydan syml). Dylen nhw weithio mewn parau i fraslunio diagram cylched sy'n cynnwys dau fylb, un ger switsh yn yr "orsaf anfon" ac un ymhellach i ffwrdd ar wifrau hir mewn rhan arall o'r ystafell neu y tu ôl i raniad (e.e. pentwr o lyfrau) yn yr "orsaf dderbyn". Ar ôl paratoi eu cylchedau, dylent sicrhau nad ydynt yn gallu gweld bylbiau ei gilydd pan fyddant yn eistedd wrth eu gorsafoedd (gweler ffigur 1).

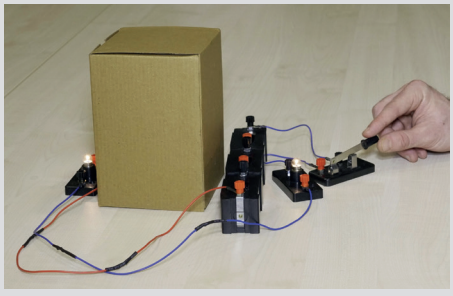
Dylech dderbyn unrhyw gyfuniad cyfresol neu gyfochrog sy'n gweithio, cyhyd â bod digon o wifrau i'w adeiladu.

FFIGUR 1:
CYFATHREBU UN FFORDD

Diagramau cylchedau ar gyfer cyfathrebu un ffordd

Top: Cylched gyfresol **Gwaelod:** Cylched gyfochrog





Llun: Cylched gyfathrebu un ffordd ar waith

GWEITHGAREDD STEM 3
NODIADAU'R ATHRO
CYFATHREBU

raf100schools.org.uk

Ar ôl iddynt gwblhau eu dolen gyfathrebu un ffordd, gall myfyrwyr ei threialu drwy amgodio negeseuon gan ddefnyddio'r olwyn cod Morse (ar eu Templed Dryswr) a'u hanfon at eu partner drwy droi'r gylched ymlaen ac i ffwrdd. Eglurwch nad oes disgwyl iddyn nhw ddod yn arbenigwyr cod Morse; y nod yw treialu'r gylched a dylent ganolbwyntio ar anfon geiriau unigol yn hytrach na negeseuon cyfan (mae anfon negeseuon hir yn gallu cymryd llawer o amser).

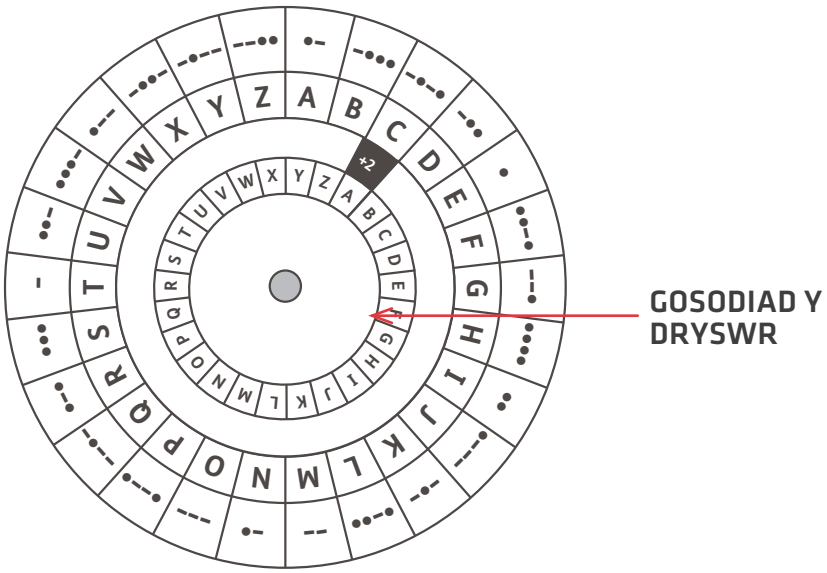
Ar eu hymgais gyntaf, maen nhw'n debygol o amgodio geiriau fel llif di-dor o smotiau a dashiau heb fylchau rhwng y llythrennau. Gadewch iddyn nhw ddarganfod yr anawsterau eu hunain ac anogwch nhw i ddatblygu eu "protocolau" amgodio eu hunain (e.e. gallent aros ychydig eiliadau rhwng pob llythyren, neu anfon dash hir iawn i wahanu'r llythrennau). Ar ôl anfon, dylent newid seddi gyda'u partner ac ymarfer derbyn a dadgodio.

Er bod troi neges i God Morse yn ei gwneud yn haws i'w hanfon, cofiwch bwysleisio nad ydy hynna'n golygu ei bod yn ddiogel. Roedd gan y ddwy ochr yn yr Ail Ryfel Byd arbenigwyr ar godio a dadgodio Morse. Mae angen amgryptio er mwyn cyfathrebu'n ddirgel. Gofynnwch iddyn nhw adeiladu dryswr (gweler ffigur 2) a'i ddefnyddio i amgryptio'u negeseuon cyn eu hamgodio a'u hanfon. Yn olaf, caiff myfyrwyr eu herio i addasu dyluniad eu cylched fel y gallan nhw anfon a derbyn negeseuon dirgel heb newid seddi (gweler ffigur 3).

FFIGUR 2:
Y DRYSWR

Gall myfyrwyr greu dryswr drwy dorri'r ddwy olwyn ar eu Templed Dryswr. Dylen nhw ddechrau drwy osod y dryswr ar +2 a'i ddefnyddio i orffen amgryptio'r llythrennau "RAF" cyn rhoi cynnig ar eu geiriau a'u gosodiadau nhw'u hunain.

Neges	R	A	F
Neges wedi'i hamgryptio	T	C	H
Neges wedi'i hamgryptio a'i hamgodio	-	-•-•	••••

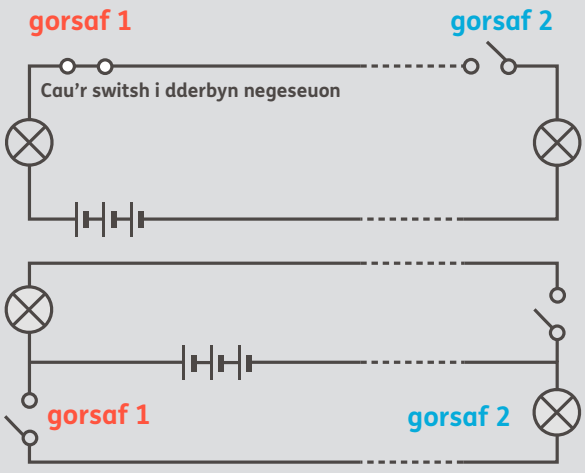


FFIGUR 3:
CYFATHREBU DWY FFORDD

Dyluniadau cylchedau ar gyfer cyfathrebu dwy ffordd.

Top: Cylched gyfresol

Gwaelod: Cylched gyfochrog



GWEITHGAREDD STEM 3
NODIADAU'R ATHRO
CYFATHREBU

RAF 100

raf100schools.org.uk

GWYBODAETH AM SIGNALAU TRYDANOL A SEIFFRAU

Yn dibynnu ar oedran a gallu'r myfyrwyr, gallech drafod rhagor ar fanteision defnyddio cod Morse i gyfathrebu dros bellteroedd maith a gwahanol ffyrdd o amgryptio negeseuon.

Yn ogystal â bod yn hawdd i'w amgodio (gyda switsh syml), a'i amgryptio (un llythyren ar y tro), mantais cod Morse oedd bod modd ei anfon fel signal digidol (gweler ffigur 4). Mae pob signal yn gwanhau wrth deithio; mewn systemau yn y ddaear, gwrthiant trydanol y ceblau sydd ar fai, ac mewn systemau di-wifr mae tonfeddi radio yn diffreithio wrth iddyn nhw deithio. Ar eu taith o'r anfonwr i'r derbynnydd, maen nhw'n debygol o godi signalau eraill, neu sŵn, hefyd (e.e. siffrwd a hisian ar orsafoedd radio analog).

Mantais dulliau amgodio digidol fel Morse yw bod sŵn yn is mewn osgled na'r cyflyrau 'ymlaen' (y smotyn neu'r dash) gan amlaf. Mae'n haws nodi a gwahanu'r signal na mewn signal analog. (Gall myfyrwyr ymchwilio i hyn drostynt eu hunain drwy roi eu llaw'n dynn dros eu ceg ac yna dweud gair wrth eu partner yn eu llais arferol. Yna, eto gyda'u llaw ar eu ceg, defnyddio "blipiau" o wahanol hyd i sillafu gair mewn cod Morse; dylent gasglu mai cyfathrebu'n ddigidol sy'n sicrhau bod y neges yn cael ei chyfleu'n fwyaf clir pan fydd y signal yn wan.

Yn ystod yr Ail Ryfel Byd roedd hi'n gymharol hawdd rhyng-gipio negeseuon y gelyn. Roedd modd codi negeseuon di-wifr ar dderbynnydd radio ac roedd modd rhyng-gipio negeseuon a anfonwyd i lawr ceblau trydanol drwy fonitro'r maes magnetig o amgylch y cebl.

Roedd pa mor ddiogel oedd y neges yn dibynnu ar y dechneg amgryptio, neu'r seiffr, a ddefnyddiwyd. Un o'r technegau amgryptio symlaf yw seiffr shift neu Cesar, lle mae'r llythrennau gwreiddiol yn cael eu disodli gan lythyren sy'n cyfateb i nifer penodol o lythrennau i fyny neu i lawr yr wyddor. Dim ond 25 o seiffrau shift gwahanol sy'n bosibl (sy'n cyfateb i osodiad +1 i +25 ar eu dryswyr). Mae hyn yn golygu eu bod yn hawdd eu datrys. Y cyfan sydd angen ei wneud yw rhoi cynnig ar bob posibilrwydd yn ei dro.

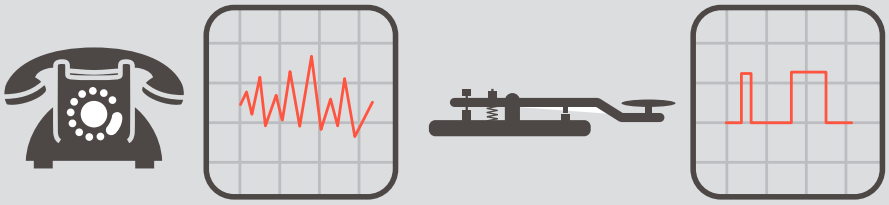
Dull amgryptio mwy diogel yw defnyddio system lle mae unrhyw lythyren yn gallu cael ei chynrychioli gan un arall, heb fod mewn unrhyw drefn arbennig. Mae modd creu'r seiffrau amnewid hyn drwy ddefnyddio cymal allweddol. Er enghraifft, i ddefnyddio ROYAL AIR FORCE fel cymal allweddol, dechreuwch drwy ddileu unrhyw fylchau a llythrennau sy'n cael eu hailadrodd (ROYALIFCE) ac yna'i ddefnyddio ar ddechrau'r wyddor seiffr. Gweddill y wyddor seiffr yw'r llythrennau sy'n weddill, yn y drefn gywir, gan ddechrau lle mae'r cymal allweddol yn gorffen (gweler ffigur 5).

FFIGUR 4:
FFÔN V TELEGRAFF

Gellir anfon negeseuon ar hyd ceblau trydanol dros y ffôn neu delegraff.

Chwith: Mae siarad i mewn i'r ffôn yn troi'r neges yn signal analog.

Dde: Mae tapio'r neges mewn cod Morse gan ddefnyddio switsh telegraff yn creu signal digidol.



FFIGUR 5: SYSTEMAU SEIFFR

SEIFFR SHIFT (GOSODIAD DRYSWR +3)

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

SEIFFR AMNEWID (CYMAL ALLWEDDOL **ROYAL AIR FORCE)**

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

Top: Enghraifft o seiffr shift. Mae'r llythrennau yn nhrefn yr wyddor.

Bottom: Enghraifft o seiffr amnewid mwy cyffredinol. Nid yw'r llythrennau yn nhrefn y wyddor mwyach.

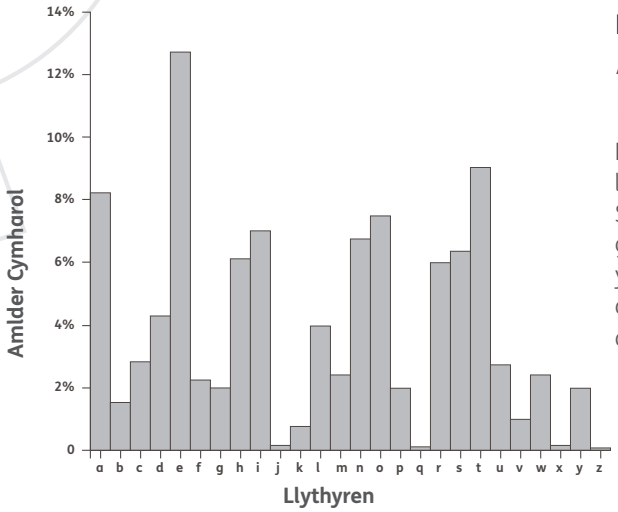
CYFATHREBU

Mae nifer y seiffrau amnewid posibl yn fawr iawn (tua 10^{26}), sy'n golygu ei bod hi'n amhosib i'r gelyn wirio pob posibilrwydd. Er hynny, mae modd datrys seiffrau amnewid drwy dechneg o'r enw dadansoddiad amlder sy'n dibynnu ar y ffaith fod rhai llythrennau'n ymddangos yn amlach nag eraill. Er enghraifft, yn Saesneg, E yw'r llythyren fwyaf cyffredin, yna T ac yna A (gweler ffigur 6). Drwy gymharu pa mor aml mae llythrennau'n codi yn y neges wedi'i hamgryptio gyda'r rheini mewn darn hir o destun plaen, mae modd adnabod y rhan fwyaf o'r llythrennau.

I ddiogelu rhag dadansoddiad amlder, byddai'r ddwy ochr yn defnyddio peiriannau i amgryptio negeseuon. Roedd Prydain yn defnyddio'r peiriant Typex. Roedd yr Almaenwyr yn defnyddio'r Enigma. Y rhan annatod o'r peiriannau seiffr hyn oedd y rotor electrofecanyddol, sef fersiwn electronig o ddryswr y myfyrwyr. Roedd pob rotor yn ddisg a oedd yn symud gyda dryswch o wifrau'n cysylltu â bysellfwrdd a lampfwrdd drwy blygfwrdd. Pe bai llythyren yn cael ei phwyso ar y bysellfwrdd, byddai'r gylched yn cynnwys y rotorau'n achosi i lythyren wahanol oleuo ar y lampfwrdd i ddangos pa destun seiffr i'w ddefnyddio. Ar ôl amgryptio pob llythyren, byddai'r rotor yn symud ymlaen un lle, felly pe bai'r un llythyren yn cael ei phwyso eto, byddai'n cael ei hamgryptio fel un wahanol.

Gwendid amlwg defnyddio un rotor yw bod y patrwm amgryptio'n cael ei ailadrodd ar ôl amgryptio 26 llythyren (gall myfyrwyr weld hyn drostynt eu hunain drwy ddefnyddio'u dryswr). Roedd y peiriannau seiffr a ddefnyddiwyd yn yr Ail Ryfel Byd yn cyflogi llawer o ddryswyr i'w gwneud yn fwy diogel (gweler ffigur 7).

Roedd gosodiadau dechrau'r rotor a'r plygfwrdd yn cael eu newid bob hyn a hyn, a oedd yn golygu bod dadgryptio'r neges symlaf yn gallu bod yn dasg amhosib bron i ddatryswyr codau gyda phen a phapur. Ni wnaeth yr Almaenwyr fyth llwyddo i ddatrys amgryptiad peiriant Typex Prydain ac roedd rhaid defnyddio'r cyfrifiadur cyntaf i ddatrys Enigma'r Almaenwyr.



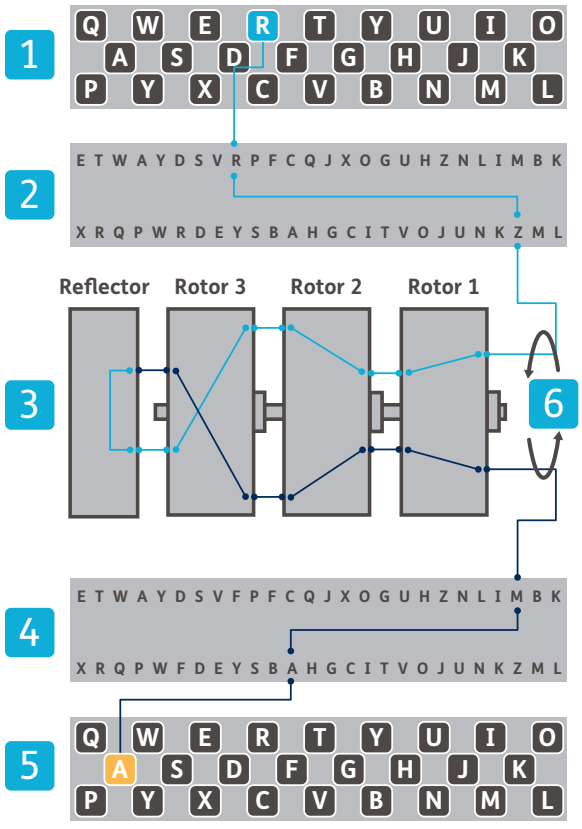
FFIGUR 6:
AMLDER LLYTHRENNAU

Dosbarthiad nodweddiadol llythrennau mewn testun Saesneg. Nid yw seiffrau gwan yn celu'r dosbarthiad yn ddigon da, a gallai datryswr codau fanteisio ar hyn i ddatgelu'r neges.

FFIGUR 7:
PEIRIANT ENIGMA

Y broses amgryptio a'r llwybr signalau drwy beiriant Enigma tri rotor yr Almaenwyr (roedd peiriant Typex pum rotor Prydain yn gweithio mewn ffordd debyg).

1. Mae'r anfonwr yn teipio llythyren ar fysellfwrdd cyffredin.
2. Mae'r signal yn cael ei anfon drwy blygfwrdd sy'n newid llythrennau o gwmpas.
3. Mae tri rotor, pob un wedi'i wifro fel spaghetti, yn newid y llythyren allbwn cyn bod adlewyrchydd yn anfon y signal drwy'r rotorau eto.
4. Mae'r signal yn pasio drwy'r plygfwrdd eto.
5. Mae'r llythyren i'w defnyddio ar gyfer amgryptio yn goleuo ar y lampfwrdd.
6. Mae'r rotor yn symud ymlaen un lle (mae safle'r rotor cyntaf yn newid wrth wasgu pob allwedd, yr ail ar ôl pwyso 26 allwedd a'r trydydd ar ôl pwyso 676 allwedd).



GWEITHGAREDD STEM 3
NODIADAU'R ATHRO
CYFATHREBU

raf100schools.org.uk

GWAITH ESTYNEDIG: DATRYS CODAU

Fel gweithgaredd estynedig gall myfyrwyr ymchwilio i wahanol ffyrdd o dorri neges wedi'i hamgryptio.

Bydd pob myfyriwr angen copi o'r daflen gwaith estynedig STEM a'r papur ysgrifennu ychwanegol. Dylent ddechrau drwy dorri'r amgryptiad ar gyfer y neges wedi'i rhyng-gipio a roddir (gweler ffigur 8).

Eglurwch fod adroddiadau tywydd yn ffynhonnell wybodaeth dda ar gyfer datryswyr codau, gan eu bod yn rhoi cyfle iddyn nhw geisio rhoi amcan synhwyrol i rai o'r geiriau. Yna dylai myfyrwyr ddewis eu gosodiad eu hunain ar gyfer y dryswr a gair yn ymwneud â'r tywydd ac yna'i amgryptio, cyn cyfnewid geiriau gyda'u partner a rasio'n erbyn ei gilydd i ddatrys amgryptiad y naill a'r llall.

Yna dylai myfyrwyr roi cynnig ar ddadansoddiad amlder (o seiffr shift). Rhoddir neges fer wedi'i hamgryptio; dylent geisio datrys yr amgryptiad drwy ganfod pa lythyren sy'n cynrychioli E (gweler y ffigur 9). Yn olaf, dylent ddewis cymal a defnyddio'r dryswyr i'w amgryptio; gan gynyddu gosodiad y dryswr unwaith ar ôl amgryptio pob llythyren. Dylent ddod i'r casgliad bod defnyddio dryswyr sy'n troi yn golygu nad yw pob llythyren yn cyfateb i'r un llythyren bob tro (ac felly does dim modd datrys yr amgryptiad drwy ddadansoddiad amlder yn unig).

CREU'R CYSYLLTIAD Â HANES

Nod y gweithgaredd cysylltiedig â hanes yw dangos sut roedd technoleg yn cael ei defnyddio yn y gorffennol. Mae'r gweithgaredd hanes yma am y torwyr codau yn Bletchley Park. Am wybodaeth am sut i ddefnyddio'r gweithgaredd estynedig STEM fel rhan o'r sesiwn hanes, trowch at y wybodaeth, nodiadau canllaw a'r syniadau ar gyfer gweithdai ar gyfer Hanes.

FFIGUR 8: DADGRYPTIO NEGESEUON AM Y TYWYDD

Neges wedi'i rhyng-gipio	**U**	**D**	**L**	**Q**
Neges wedi'i dadgryptio	**R**	**A**	**I**	**N**
Gosodiad y dryswr	**+3**			

Gosodiad y dryswr	**+6**			
Neges	S	N	O	W
Neges wedi'i hamgryptio	**A**	**T**	**U**	**C**

Chwith: Mae llythyren olaf (N) y neges wedi'i rhyng-gipio wedi'i rhoi iddyn nhw. Mae hyn yn cyfateb i osodiad o +3 ar y dryswr, a gallant ei ddefnyddio i ddadgryptio gweddill y neges i RAIN.

Dde: Dylai myfyrwyr ddewis eu gair eu hunain sy'n ymwneud â'r tywydd (e.e. SNOW) a'i amgryptio gan ddefnyddio'u gosodiad cyfrin eu hunain (ee **+6**) cyn rhoi'r neges i'w partner i weld os gallan nhw dorri'r amgryptiad.

FFIGUR 9: DADANSODDIAD AMLDER A DRYSWYR SY'N TROI

Neges wedi'i hamgryptio	O	**A**	J	Z		I	**A**	Z	E	Y	W	H		O	Q	L	L	H	E	**A**	O
Neges wedi'i dadgryptio	S	**E**	N	D		M	**E**	D	I	C	A	L		S	U	P	P	L	I	**E**	S

Neges	**S**	E	N	D	-	A	I	R	-	**S**	U	P	P	O	R	T
Gosodiad dryswr	**+2**	+3	+4	+5	-	+6	+7	+8	-	+9	+10	+11	+12	+13	+14	+15
Neges wedi'i hamgryptio	**U**	H	R	I	-	G	P	Z	-	**B**	E	A	B	B	F	I

Top: Y llythrennau sy'n codi amlaf yn y neges wedi'i hamgryptio a roddir yw A ac O. Ar ôl rhywfaint o brofi a methu, neu feddwl, dylen nhw sylweddoli mai'r llythyren A sydd fwyaf tebygol o gynrychioli E, sy'n cyfateb i osodiad o **+4** ar y dryswr. Felly mae A yn dod yn E, mae B yn dod yn F, ac ati.

Gwaelod: Dylai'r myfyrwyr ddewis eu brawddeg tri neu bedwar gair eu hunain (e.e. SEND AIR SUPPORT) a'u gosodiad cychwynnol nhw'u hunain (e.e. +2) ac amgryptio'r neges drwy gynyddu gosodiad y dryswr un lle ar ôl pob llythyren. Yn wahanol i seiffr amnewid cyffredin, dylent weld bod hyn yn golygu nad yw pob llythyren yn cyfateb yn uniongyrchol i un arall (yn yr enghraifft a roddir, caiff S ei chynrychioli gan U a B).

RHAGOR O WYBODAETH

Er mwyn dysgu mwy am sut mae gwyddonwyr yn elwa ar fecaneg cwantwm i gyfathrebu ac amgryptio, gweler **bit.ly/RAF-Qubit**. Er mwyn dysgu mwy am addysgu cylchedau trydan, gweler Cefnogi Addysgu Ffiseg (11-14): **bit.ly/RAF-Circuits**.