DATRYS CODAU

raf100schools.org.uk

CYFLWYNIAD

Ers canrifoedd, mae rhai pobl, sefydliadau a llywodraethau wedi bod angen anfon gwybodaeth yn gyfrinachol. Mae gwahanol ffyrdd o anfon negeseuon yn ddirgel wedi'u datblygu dros amser ond y dull mwyaf cyffredin yw celu gwybodaeth drwy ddefnyddio cod neu seiffr (gweler y bocs isod).

Yn yr un modd ag y mae rhai pobl eisiau cadw eu negeseuon i bobl benodol yn gyfrinach, mae eraill eisiau gwybod beth yw'r gyfrinach! Felly, wrth i bobl ddatblygu codau a seiffrau i anfon negeseuon yn gyfrinachol, bydd eraill yn treulio'u hamser yn ceisio'u datrys. Weithiau byddai'r negeseuon yn cael eu hanfon ar ddarnau o bapur ac weithiau byddai'n rhaid i bobl eu cofio. Gallai negeseuon a anfonwyd yn gyfrinachol fod yn unrhyw beth o lythyron serch i ddarganfyddiadau technoleg newydd ond, ar adeg rhyfel ac yn y byd milwrol, maen nhw wir yn gallu newid bywydau.

I lywodraethau yn ystod rhyfel, mae cadw eu cyfathrebu'n gyfrinachol yn bwysig tu hwnt, a gall y negeseuon hyn gynnwys gwybodaeth rhwng llywodraethau cyfeillgar, negeseuon i arweinwyr y fyddin yn rhoi gorchmynion i ymosod, neu geisiadau am fwy o gyflenwadau. Gall cipio neu ryng-gipio neges sy'n cael ei hanfon yn gyfrinachol ddatgelu gwybodaeth bwysig i'r ochr arall. Gallai fod yn rhywbeth o bwys, fel pryd mae byddin yn bwriadu dechrau brwydr, neu gallai fod yn rhywbeth sy'n ymddangos yn ddibwys, fel prinder bara - ond mae'r cyfan yn datgelu agwedd bwysig ar sut mae un ochr yn ymdopi neu'n cynllunio.

Mae llywodraethau wedi sefydlu sefydliadau arbennig – asiantaethau cudd-wybodaeth neu ysbiwyr – i ryng-gipio negeseuon ond os yw'r neges wedi'i hamgodio, mae angen pobl sy'n gallu datrys neu dorri'r seiffr. Mae datrys seiffr neu god yn datgelu ystyr y neges – fodd bynnag, rhaid casglu sawl darn o wybodaeth i greu darlun llawn er mwyn deall gwir arwyddocâd y neges. Mae hynny'n golygu bod rhaid i grŵp cudd-wybodaeth a grŵp datrys codau ryng-gipio, datrys a dadansoddi cannoedd o negeseuon i wneud defnydd iawn a phriodol o wybodaeth yn ystod rhyfel.

Cod dirgel	Dull o gelu ystyr neges drwy newid geiriau cyfan, a defnyddio geiriau eraill yn eu lle neu ddefnyddio symbol gwahanol, fel delweddau. Ar y môr gall baneri gael eu defnyddio yn lle geiriau a brawddegau
amgodio	Neges sydd wedi'i hysgrifennu mewn cod
seiffr	Yn dibynnu ar gelu neges drwy gymysgu llythrennau unigol y neges
amgryptio	Anfon neges gyfan â'r llythrennau wedi cymysgu gan ddefnyddio seiffr
dadgryptio	Gwybod beth yw'r seiffr ar gyfer datgelu neges wedi'i hamgryptio, e.e. gwybod bod pob llythyren wedi cael ei disodli gan yr un nesaf ati yn y wyddor
seiffr Cesar	Dull o gelu neges drwy gymysgu'r llythrennau drwy symud pob un ar hyd y wyddor, e.e. a = c, b=d, c=e, ac ati.
brawddeg allweddol/ allweddair/crib	Sut mae canfod sut mae seiffr amnewid wedi cymysgu'r llythrennau; mae'r allweddair yn rhoi ambell lythyren o'r wyddor i chi ac yna gallwch chi weithio allan y gweddill
Datrys	Datrys neges sydd wedi'i hamgryptio
Cryptddadansoddwr	Rhywun sy'n astudio negeseuon dirgel er mwyn cael gafael ar wybodaeth wedi'i hamgryptio.
Dadansoddwr cudd-wybodaeth	Rhywun sy'n darllen drwy'r holl wybodaeth sydd wedi'i chasglu o negeseuon dirgel ac o ffynonellau agored i geisio gweld beth sy'n wir ac a oes unrhyw batrymau yn y wybodaeth, ac sydd wedyn yn gorfod argymell camau gweithredu

DATRYS CODAU

RAF 100

raf100schools.org.uk

Peiriant Enigma	Peiriant a ddefnyddiwyd gan luoedd yr Almaen yn ystod yr Ail Ryfel Byd i amgryptio'r holl negeseuon a anfonwyd drwy radio neu delegraff trydan
Peiriant Bombe	Peiriant a gafodd ei ddyfeisio i weithio allan sut mae dadgryptio neges a gafodd ei hamgryptio gan beiriant Enigma
Gorsaf Y	Lle yn y DU ag erial mawr a oedd yn clustfeinio ar negeseuon dirgel wedi'u hamgryptio a oedd yn cael eu hanfon gan yr Almaenwyr a'u cynghreiriaid, yn eu hysgrifennu ac yna'u hanfon i safleoedd cudd-wybodaeth yn y DU i'w dadgryptio
Peiriant Lorenz	Peiriant ar gyfer anfon negeseuon wedi'u hamgryptio a oedd hyd yn oed yn fwy soffistigedig na'r peiriant Enigma

CODAU A SEIFFRAU

Ym maes cyfathrebu cyfrinachol (cryptograffeg), mae cod yn cyfeirio at ffordd o gelu ystyr neges drwy newid geiriau cyfan. Er enghraifft, yn ystod yr Ail Ryfel Byd, roedd y Cynghreiriaid yn defnyddio'r gair 'DYNAMO' wrth gyfeirio at yr ymgyrch i achub milwyr o draeth Dunkirk. Ar y llaw arall, mae seiffr yn dibynnu ar gelu neges drwy gymysgu llythrennau unigol y neges.

Er enghraifft, mae modd celu'r gair 'DYNAMO' drwy newid pob llythyren gyda'r un nesaf yn y wyddor, felly ar ôl ei amgryptio bydd yn ymddangos fel 'EVOLJSL'.

Yn y ddau Ryfel Byd, roedd pob ochr yn dibynnu'n bennaf ar ddefnyddio seiffrau yn hytrach na chodau, oherwydd gyda seiffrau, y cyfan roedd angen i'r sawl a oedd yn anfon a derbyn y neges ei wneud oedd rhannu cyfres o gyfarwyddiadau byr y gellid eu newid yn hawdd (e.e. rydw i wedi amgryptio'r neges hon drwy newid pob llythyren gyda'r un sy'n ei dilyn yn y wyddor), yn hytrach na chael llyfr codau mawr gyda'r fersiynau amgen ar gyfer yr holl eiriau y gallai fod eu hangen arnyn nhw i gadw cyfrinach.

CYFATHREBU DIRGEL YN Y RHYFEL BYD CYNTAF

Yn y Rhyfel Byd Cyntaf, neu'r Rhyfel Mawr, ochr yn ochr â dulliau mwy traddodiadol, fel colomennod neges, cafodd miliynau o negeseuon eu hanfon gan ddefnyddio technoleg fodern darllediadau radio a thelegraff trydanol. Defnyddiwyd tonfeddi radio a chylchredau trydanol oherwydd bod modd anfon negeseuon dros bellteroedd maith mewn eiliadau, yn wahanol i anfon neges bapur. Fodd bynnag, byddai'n ddigon hawdd i unrhyw un allu gwrando ar neges radio neu godi negeseuon telegraff a deall beth oedd y neges. Dyma pam i lywodraethau ddechrau amgryptio'u negeseuon. Roedd rhaid cytuno ar y dechneg amgryptio (seiffr) o flaen llaw fel bod y sawl a oedd yn derbyn y neges yn gallu ei dadgryptio a deall beth oedd yn cael ei anfon ato.

Y dull amgryptio symlaf yw defnyddio 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 y wyddor. Fodd bynnag, dim ond 25 seiffr shift gwahanol sy'n bosib, felly maen nhw'n hawdd eu datrys drwy roi cynnig ar bob posibilrwydd yn ei dro. Dull amgryptio gwell yw defnyddio system lle gall unrhyw lythyren gael ei chynrychioli gan un arall heb unrhyw drefn arbennig. Mae'r seiffrau amnewid hyn yn cael eu creu drwy ddefnyddio cymal allweddol. Er enghraifft, os mai 'Royal Air Force' fyddai'r cymal allweddol, y cam cyntaf fyddai cael gwared ar unrhyw fylchau a llythrennau sy'n ymddangos fwy nag unwaith (ROYALIFCE) ac yna'i ddefnyddio ar ddechrau'r wyddor. Gweddill y wyddor seiffr yw'r llythrennau sy'n weddill, yn y drefn gywir, gan ddechrau lle mae'r cymal allweddol yn gorffen.

Os nad oes gan rywun y cymal allweddol, yna mae'n gallu cymryd amser maith i ddatgelu'r seiffr, gan fod biliynau o bosibiliadau. Mae pobl yn ceisio datrys seiffr fel hwn drwy ddefnyddio dadansoddiad amlder. Mae pob iaith yn defnyddio rhai llythrennau fwy nag eraill; yn Saesneg er enghraifft, y llythyren E yw'r un fwyaf cyffredin, yna T ac yna A. Drwy gymharu pa mor aml mae llythrennau'n ymddangos yn y neges wedi'i hamgryptio o gymharu â darn hir o destun plaen, mae modd adnabod y rhan fwyaf o'r llythrennau. Enw arall am allweddair/cymal allweddol yw 'crib'.

DATRYS CODAU

raf100schools.org.uk

YSGOL COD A SEIFFR Y LLYWODRAETH

Ym 1909, sefydlodd Llywodraeth Prydain y Gwasanaeth Cudd-wybodaeth Dirgel (Secret Intelligence Service, neu Bureau ar y pryd). Roedd SIS yn ymwneud â phob math o waith casglu cudd-wybodaeth, datrys codau a dadansoddi gwybodaeth. Hefyd, yn ystod y Rhyfel Byd Cyntaf, roedd gan y Fyddin a'r Llynges eu hunedau cudd-wybodaeth eu hunain a oedd yn rhyng-gipio a dadgryptio negeseuon. Ar ôl y rhyfel, cafodd Hugh Sinclair, Cyfarwyddwr Cudd-wybodaeth y Llynges, y dasg o uno unedau'r Fyddin a'r Llynges a chreu Ysgol Cod a Seiffr y Llywodraeth. Penodwyd Sinclair yn bennaeth SIS hefyd. Roedd yr unedau cudd-wybodaeth hyn i gyd wedi'u lleoli yn Llundain.

Yn ystod y 1920au a'r 1930au, cynyddodd nifer y staff yn yr Ysgol ac fe ddechreuon nhw ddysgu am y dulliau newydd o amgryptio negeseuon a oedd yn cael eu datblygu. Roedd recriwtio datryswyr codau wedi targedu ieithyddion hyd yma: y rhai oedd â gafael dda ar ieithoedd (yn enwedig gan y byddai'r negeseuon a ryng-gipiwyd, ar ôl eu dadgryptio, yn dal i fod mewn iaith dramor). Fodd bynnag, roedd newidiadau technolegol yn y cyfnod hwnnw'n golygu bod y negeseuon a oedd yn cael eu hanfon yn ymddangos fel bod ganddynt seiffrau mwy cymhleth o lawer na'r rhai yr oedd pobl yn gyfarwydd â nhw - roedd hi'n amlwg bod rhyw fath o beiriant yn cael ei ddefnyddio i greu seiffr. Penderfynodd Sinclair ddechrau recriwtio mathemategwyr yn ogystal ag ieithyddion i'w dîm.

Ym 1938, roedd digwyddiadau ledled Ewrop yn awgrymu bod rhyfel arall ar y gorwel. Penderfynodd Sinclair y gallai fod yn beryglus cael ei bobl bwysig i gyd yn Llundain, gan y byddai'r ddinas yn debygol o ddioddef ymosodiadau o'r awyr mewn unrhyw ryfel, fel y digwyddodd yn y Rhyfel Byd Cyntaf. Felly, yn dawel bach aeth y llywodraeth ati i brynu neu feddiannu (atafael) nifer o blastai yn y siroedd o amgylch Llundain. Un o'r plastai allweddol oedd Bletchley Park ym mhentref Bletchley, Swydd Buckingham, ar gyrion Llundain. Roedd y safle'n ddelfrydol gan fod digon o le yno a'i fod yn agos i orsaf drenau lle'r oedd trenau'n teithio'n syth i Lundain. Symudodd yr Ysgol gyfan i Bletchley ym 1938 o dan arweiniad Alastair Denniston.

Y PEIRIANT ENIGMA A DATRYS ENIGMA

Cafodd y peiriant Enigma ei ddyfeisio gan beiriannydd o'r Almaen, Arthur Scherbius, yn fuan wedi'r Rhyfel Byd Cyntaf.

Roedd y peiriant yn edrych fel teipiadur a chynhyrchwyd sawl fersiwn ohono. Roedd ganddo lampfwrdd uwchben y bysellau, gyda lamp ar gyfer pob llythyren. Roedd y gweithredwr yn pwyso'r fysell ar gyfer llythyren testun plaen y neges a byddai'r llythyren wedi'i hamgryptio'n goleuo ar y lampfwrdd. Fe'i mabwysiadwyd gan luoedd arfog yr Almaen rhwng 1926 a 1935. Roedd y peiriant yn cynnwys cyfres o rotorau cyfnewidiadwy, a oedd yn troi bob tro y byddai bysell yn cael ei phwyso fel bod y seiffr yn newid drwy'r amser. I gyd-fynd â hyn roedd plygfwrdd ar flaen y peiriant, lle'r oedd parau o lythrennau'n cael eu had-drefnu. Roedd y ddwy system hyn gyda'i gilydd yn cynnig 159 miliwn miliwn miliwn o osodiadau posibl i ddewis o'u plith. A dyna pam y credai'r Almaenwyr ei bod hi'n amhosibl datrys Enigma.

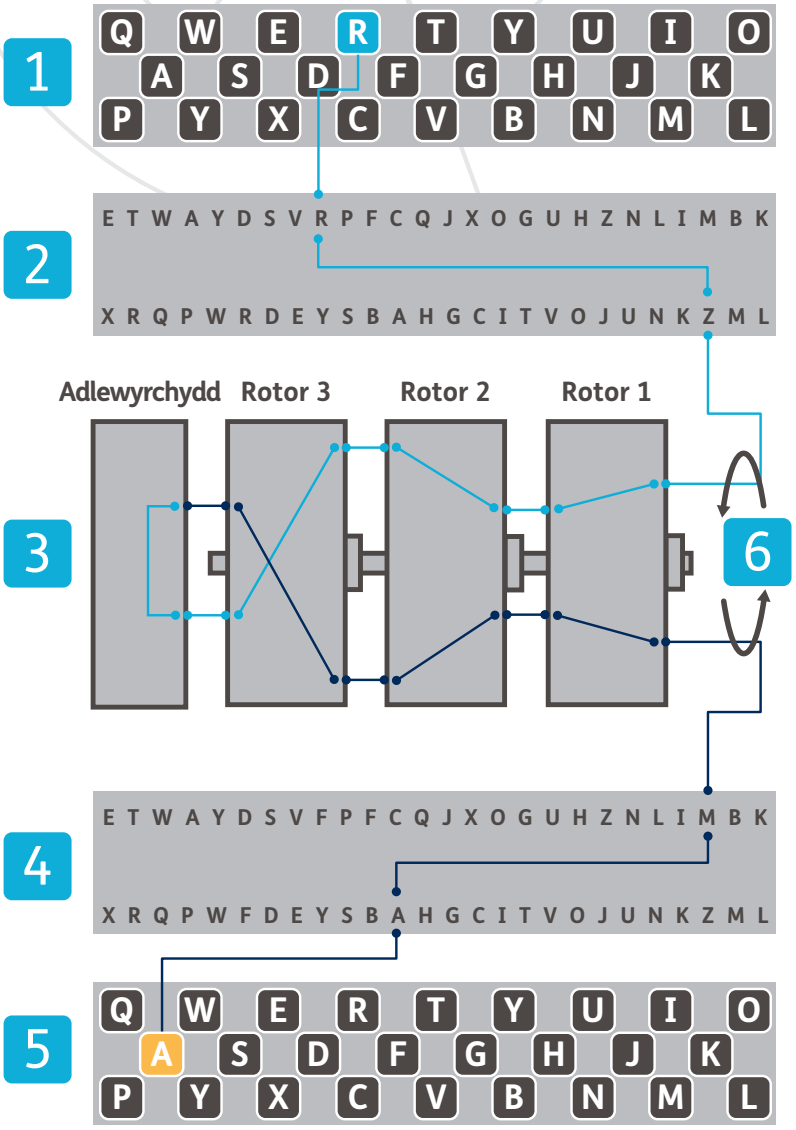
Roedd y Pwyliaid wedi datrys Enigma mor gynnar â 1932, ond ym 1939, gyda rhyfel ar y gorwel, penderfynodd y Pwyliaid ddweud wrth Brydain am eu llwyddiannau. Roedd Dilly Knox, un o ddatryswyr codau Prydain yn y Rhyfel Byd Cyntaf, yn sicr y gallai dorri'r system, ac aeth ati i sefydlu Gorsaf Ymchwil Enigma – sef fe a Tony Kendrick i ddechrau gyda Peter Twinn, Alan Turing a Gordon Welchman yn ymuno â'r tîm maes o law. Roeddent yn gweithio yn iard y stablau yn Bletchley Park, a dyma lle'r oedd y negeseuon Enigma cyntaf yn ystod y rhyfel yn cael eu datrys ym mis Ionawr 1940. Parhaodd negeseuon Enigma i gael eu datrys yn rheolaidd yn Bletchley Park gydol y rhyfel.

Detholiad o'r Bletchley Park Trust

DATRYS CODAU

RAF 100

raf100schools.org.uk



Y PEIRIANT ENIGMA

Y broses amgryptio a'r llwybr signalau drwy'r peiriant Enigma.

1. Mae'r anfonwr yn teipio llythyren ar fysellfwrdd cyffredin.
2. Mae'r signal yn cael ei anfon drwy blygfwrdd sy'n symud 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 bwyso pob bysell, yr ail ar ôl pwyso 26 bysell a'r trydydd ar ôl pwyso 676 bysell).

Y broblem i'r tîm yn Bletchley oedd bod angen iddyn nhw dorri cannoedd o negeseuon Enigma a oedd yn dod i mewn bob dydd yn gyflym. Arweiniodd hynny at adeiladu'r peiriant Bombe.

DATRYS CODAU

raf100schools.org.uk

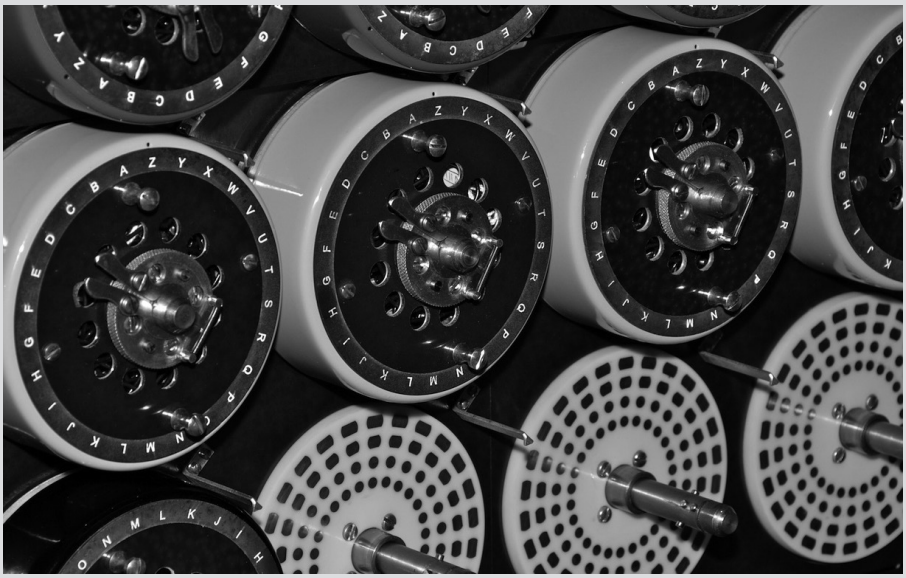
TURING-WELCHMAN BOMBE

Ar sail y wybodaeth a gyflwynwyd gan y Pwyliaid, datblygodd Alan Turing, y mathemategydd o Brydain, beiriant a oedd yn gallu ail-greu lleoliad y bysellau. Enw'r peiriant oedd y Bombe (y Turing-Welchman Bombe yn ddiweddarach) ac fe'i hadeiladwyd gan y British Tabulating Machine Company (BTM) yn Letchworth, Swydd Hertford o dan oruchwyliaeth Harold (Doc) Keen.

Roedd yr enw'n dod o Bomba, peiriant tebyg a gafodd ei ddatblygu gan y Pwyliaid toc cyn dechrau'r Ail Ryfel Byd.

Dyluniodd Turing y Bombe Prydeinig ym 1939. O gymharu â Bomba'r Pwyliaid, roedd e'n defnyddio dull hollol wahanol. Roedd yn seiliedig ar y dybiaeth bod crib hysbys yn bresennol mewn man penodol yn y neges. Cyrhaeddodd y peiriant cyntaf, o'r enw 'Victory', Bletchley Park ar 18 Mawrth 1940.

Cafodd y Bombe ei wella ymhellach gan y bwrdd lletraws, a ddyfeisiwyd gan ddatryswr codau arall, Gordon Welchman. Roedd y bwrdd yn golygu bod modd datrys codau mewn llai o lawer o gamau. Gosodwyd Bombe arall, yn cynnwys bwrdd lletraws Welchman,



ar 8 Awst 1940. Ei enw oedd 'Agnus Dei', a gafodd ei fyrhau i 'Agnes' neu 'Aggie' maes o law. Cafodd y peiriant cyntaf (Victory) ei addasu'n ddiweddarach gyda bwrdd lletraws hefyd.

Yn ystod y rhyfel, adeiladwyd 200 a mwy o'r Turing-Welchman Bombes. Er mwyn osgoi'r risg o'u colli mewn ymosodiad â bomiau, fe'u gwasgarwyd rhwng Bletchley Park a'i is-orsafoedd yn Wavendon, Adstock, Gayhurst, Eastcote a Stanmore, lle cawsant eu gweithredu gan WRNS, technegwyr yr RAF a phersonél sifilaidd.

Detholiad o'r Crypto Museum **www.cryptomuseum.com/crypto/bombe/**

Felly, diben y Bombe oedd ceisio dod o hyd i'r crib yn y neges. Ar ôl dod o hyd i'r crib, roedd modd cyfyngu ar nifer y gosodiadau posibl a oedd wedi amgryptio'r neges ar y peiriant Enigma, er mwyn ceisio dadgryptio'r neges gyfan.

Roedd y crib ar ddechrau'r neges gan amlaf ac roedd o gymorth i ddweud wrth y derbynnydd ei fod yn defnyddio'r gosodiadau cywir ar ei beiriant.

Llyfrau seiffrau: Rhoddwyd llyfrau seiffrau i filwyr yr Almaen a oedd yn dweud wrthynt pa seiffr i'w ddefnyddio ar eu peiriant ar ddiwrnod penodol. Roedd y llyfrau'n cael eu newid bob wythnos, ac eithrio ar gyfer y rhannau hynny o'r lluoedd arfog y byddai'n anodd iawn cael llyfrau seiffrau newydd atynt. Byddai llongau tanfor yn defnyddio'u llyfrau seiffrau am wythnos, gan eu bod o dan y dŵr am gyfnodau hir yn aml. Roedd cipio llyfrau seiffrau yn fuddiol iawn, gan eu bod yn rhoi'r crib ar gyfer diwrnod arbennig ac ar gyfer negeseuon penodol - e.e. holl negeseuon y Luftwaffe ar 2 Tachwedd 1943. O wybod y crib, gallai'r datryswyr codau roi eu peiriant Enigma ar y gosodiadau cywir ac ni fyddent angen y peiriant Bombe i wneud ei waith - a allai gymryd oriau.

DATRYS CODAU

raf100schools.org.uk

O ORSAF Y I WEITHREDU

Ar draws y DU roedd canolfannau o'r enw gorsafoedd 'Y'. Roedd yr enw 'Y' yn dod o siâp yr erial, a dyma oedd yn ei wneud yn arwyddocaol. Byddai gorsaf Y yn gwrando ar y negeseuon radio lu a oedd yn cael eu hanfon ar draws y tonfeddi. Roedd rhai'n gwrando ar negeseuon llais ond gwaith y rhan fwyaf oedd codi'r negeseuon wedi'u hamgryptio a oedd yn cael eu hanfon rhwng byddinoedd a chadlywyddion, adrannau'r llywodraeth ac ati. Byddai staff gorsaf Y (milwyr) yn casglu cannoedd o negeseuon bob dydd, a byddai'r rhain yn cael eu hanfon wedyn i lefydd fel Bletchley Park, naill ai ar bapur ar gefn beic modur neu drwy ddefnyddio peiriant telebrintiwr – math o argraffydd electronig a oedd yn argraffu neges a oedd wedi cael ei hanfon yn electronig neu i lawr llinell ffôn.

Yn Bletchley: byddai'r neges wedi'i hamgryptio yn cael ei rhoi i un o'r tîm datrys codau. Byddent yn gweithio gyda gweithredwyr y peiriant Bombe i geisio canfod y seiffr – y crib a fyddai'n helpu i roi'r gosodiadau ar gyfer peiriant Enigma. Os byddai'r Bombe yn dod o hyd i gyfatebiaeth a bod modd troi'r seiffr yn neges, byddai'r neges honno'n cael ei rhoi i'r cyfieithwyr. Byddai'r cyfieithwyr ynghlwm wrth uned filwrol neu gudd-wybodaeth. Y WRNS (Gwasanaeth Llynges Frenhinol y Menywod) oedd yn gweithredu'r peiriannau Bombe fel rheol. Roedd tîm yr RAF yn gweithio yng Nghabanau 3 a 6 gan mwyaf, gyda rhai o'r timau dadansoddi yno hefyd.

Dadansoddi: Ar ôl eu dadgryptio a chyfieithu'r negeseuon, byddent yn cael eu dadansoddi â'u cymharu â chudd-wybodaeth arall. Roedd peth o'r wybodaeth hon yn dod o negeseuon a oedd wedi'u dadgryptio yn Bletchley Park, ond roedd deunydd arall yn dod o lefydd pellach i ffwrdd ac o ffynonellau cudd-wybodaeth eraill. Roedd gan yr RAF safle ym Medmenham, canolfan yr awyrlu ar gyfer uned dehongli ffotograffau. Roedd holl ffotograffau rhagarchwilio a ffotograffau awyr yr RAF o ymgyrchoedd yn cael eu harchwilio yno. Roedd gwybodaeth a ddatgelwyd yn Bletchley yn cael ei throsglwyddo i Medmenham er mwyn cymharu trafodaethau am symudiadau milwyr â'r ffotograffau a dynnwyd, er enghraifft.

Fel arall, gallai'r dadansoddiad gael ei anfon i ganol Llundain i'w gymharu â gwybodaeth arall a oedd yn cael ei chasglu gan y SIS a'i rwydwaith rhyngwladol o ysbiwyr.

Gweithredu: Gallai dadansoddi'r wybodaeth a roddwyd gan negeseuon wedi'u dadgryptio effeithio ar benderfyniadau neu gynlluniau milwrol. Weithiau byddai'n cael effaith yn syth bin, e.e. symud rhagor o awyrennau i rannau arbennig o'r DU yn barod am ymosodiad. Weithiau gallai'r wybodaeth effeithio ar gynlluniau byddin Prydain dros gyfnod hir, e.e. sut dylid cynllunio ymosodiad ar gyfer misoedd yn y dyfodol ac ar gyfer pa ddyddiad, yn ôl yr hyn oedd gan yr Almaenwyr mewn golwg. Weithiau ni fyddai'r wybodaeth a gasglwyd yn arwain at unrhyw weithredu uniongyrchol, e.e. cyn D-Day, pan ymosododd y Cynghreiriaid ar Normandi, roedd y negeseuon wedi'u dadgryptio a'r gudd-wybodaeth ehangach a gasglwyd yn cefnogi'r farn nad oedd yr Almaenwyr yn gwybod am y bwriad i ymosod ar Normandi. Ar adegau eraill, penderfynwyd peidio â gwneud unrhyw beth ar ôl dadgryptio negeseuon rhag i'r Almaenwyr amau bod modd dadgryptio negeseuon Enigma - gallai hyn fod yn benderfyniad dadleuol yn aml, oherwydd gallai olygu bod Prydeinwyr yn colli eu bywydau yn hytrach na gweithredu ar gudd-wybodaeth.

Amserlenni: Roedd ceisio datrys y negeseuon Almaeneg a anfonwyd drwy beiriannau Enigma yn ras yn erbyn y cloc. Ofer fyddai gallu deall neges yn y pen draw os oedd yr hyn dan sylw yn y neges wedi digwydd ddiwrnodau neu wythnos ynghynt. Felly, roedd ceisio dadgryptio neges a datgelu ei hystyr yn fater o frys, ac yn ddelfrydol byddent yn ceisio gwneud hynny o fewn ychydig oriau i'r neges gyrraedd Bletchley.

DATRYS CODAU

raf100schools.org.uk

PWY OEDD YN GWEITHIO YN BLETCHLEY PARK?

Pan sefydlwyd Bletchley gyntaf ym 1938, dim ond ychydig gannoedd o bobl a oedd yn gweithio yno, ond cynyddodd y niferoedd gydag amser. Erbyn Ionawr 1945, roedd 10,000 o bobl yn gweithio yn Bletchley, tri chwarter ohonyn nhw'n fenywod. Roedd patrwm shifftiau ar waith fel bod y lle'n gallu bod ar waith 24 awr y dydd. Roedd y bobl yno, yn cynnwys y menywod, yn gweithio fel mathemategwyr, datryswyr codau, cyfieithwyr (i gyfieithu'r neges ar ôl ei dadgryptio), dadansoddwyr, gweinyddwyr a gweithredwyr peiriannau.

RÔL CUDD-WYBODAETH YN YSTOD Y RHYFEL

Pan fydd pobl yn meddwl am wrthdaro a rhyfel, y darlun sydd ganddynt fel arfer yw byddinoedd yn mynd i flaen y gad, ac er bod canfod gwybodaeth (cudd-wybodaeth) bob amser wedi bod yn bwysig, nid oedd bob amser yn cael ei hystyried mor bwysig â'r brwydro go iawn.

Newidiodd hynny yn yr Ail Ryfel Byd. Roedd pŵer y Natsïaid yn Ewrop a datblygiadau mewn technoleg yn golygu bod modd rhyfela mewn ffyrdd eraill – propaganda, cynllunio strategol, twyll a thrwy wybod beth oedd eich gelyn yn ei wneud fel y gallech chi ddylanwadu arnynt neu eu hatal.

https://bletchleypark.org.uk/cms/2017/01/0110_colossus-10-with-attending-Wren

Roedd yr RAF yn gyfrifol am filoedd o ymgyrchoedd rhagarchwilio yn ogystal â'i rôl ryfela. Roedd cannoedd o ddynion a menywod yn gweithio fel asiantiaid cudd-wybodaeth ledled Ewrop, yn casglu gwybodaeth a'i hanfon i'r DU. Yma ym Mhrydain, roedd miloedd o ddynion a menywod yn gweithio yn y fyddin fel datryswyr codau, dadansoddwyr a strategwyr ar gyfer twyll.

Yn ystod y cynllunio ar gyfer D-Day a'r ymosod ar orllewin Ewrop, defnyddiodd y Cynghreiriaid eu gwaith casglu cudd-wybodaeth i ddeall lle'r oedd milwyr yr Almaen, sut roedd modd trefnu amddiffynfeydd a pha mor gyflym y gellid eu hatgyfnerthu. Yn ogystal â'r paratoadau ar gyfer yr ymosodiad, treuliodd y Cynghreiriaid fisoedd yn anfon gwybodaeth anwir er mwyn argyhoeddi'r Almaenwyr y byddai ymosodiad yn dechrau ar safleoedd eraill ar hyd arfordir Ffrainc neu hyd yn oed yn Norwy. O'r negeseuon a gafodd eu rhyng-gipio a'u dadgryptio gan y Prydeinwyr, gallent weld nad oedd yr Almaenwyr wedi dyfalu mai Normandi fyddai targed yr ymosodiad ac roedden nhw'n sicr mai yn Calais fyddai'r ymosodiad. Roedd gwybod nad oedd yr Almaenwyr yn barod yn rhoi mantais enfawr i'r Cynghreiriaid pan ymosodon nhw'n llwyddiannus ar 6 Mehefin 1944. Dywedir bod defnyddio cudd-wybodaeth i dwyllo, yn ogystal â chlustfeinio, wedi helpu i ddod â'r rhyfel i ben yn gynt na thrwy ymladd yn unig.

DATRYS CODAU

raf100schools.org.uk

DEFNYDDIO'R WYBODAETH HON

Mae'n bosib cyfuno'r wybodaeth hanesyddol a ffeithiol hon gyda'r ffilm gyflwyno a'r adnoddau o'r adran adnoddau i ystyried rhai syniadau creadigol mewn clwb ysgol/clwb anffurfiol, neu ar gyfer gwers sy'n fwy seiliedig ar y cwricwlwm.

Isod, mae yna syniadau a chwestiynau ymholi a gallai'r deunyddiau hyn eich helpu gyda'r rhain.

Yn ogystal â'r wybodaeth hanesyddol uchod, mae astudiaethau achos a gwybodaeth ychwanegol ar gael yn yr adran adnoddau. Mae'r rhain yn cynnwys bywgraffiadau ac astudiaethau achos ar dechnoleg awyrennau.

CWESTIYNAU ALLWEDDOL I'W HARCHWILIO MEWN UNRHYW LEOLIAD:

Pam mae negeseuon dirgel a datrys codau mor bwysig yn ystod rhyfel? Pam oedd gallu deall negeseuon wedi'u hamgryptio y Natsïaid a'u cynghreiriaid yn bwysig yn ystod yr Ail Ryfel Byd?

SUT I DDEFNYDDIO'R DEUNYDD HWN MEWN CLWB HANES NEU GLWB AMSER CINIO/AR ÔL YSGOL/CLWB ANFFURFIOL

Mae'r syniadau hyn yn addas ar gyfer cymysgedd o grwpiau oedran a galluoedd. Mae'n bosibl eu defnyddio gyda map rhyngweithiol i ddechrau ymchwiliad hanes lleol hefyd.

DECHREUWCH DRWY DDANGOS Y FFILM: *CODEBREAKERS*

Rhowch y wybodaeth hanesyddol i'r myfyrwyr neu ei darllen yn uchel iddynt, a dewiswch un o'r cwestiynau neu'r ddau ohonynt o'r rhestr uchod a fyddai o ddiddordeb i'r grŵp. (Hwyrach yr hoffech ddefnyddio'r cwestiynau ychwanegol yn y bocs i sbarduno syniadau.)

Gofynnwch i'r grŵp greu neu ddyfeisio seiffr amnewid neu shift ac yna'i ddefnyddio i amgryptio negeseuon. Gallech ddefnyddio'r gweithgaredd sy'n cael sylw yn y wers isod (c) ar gyfer plant 11-13 oed hefyd.

Dewiswch rai o'r astudiaethau achos/bywgraffiadau o'r adran adnoddau. Gofynnwch i'r bobl ifanc ateb y cwestiwn (cwestiynau) a chyflwyno'u canfyddiadau ar ffurf:

- Poster gwybodaeth am Bletchley Park – mewn cod.
- Stori papur newydd ar gyfer cylchlythyr yr ysgol/grŵp ar rôl Bletchley Park yn ystod y rhyfel.
- Arddangosiad ar gyfer hysbysfwrdd yr ysgol/dosbarth/grŵp am y gwahanol bobl a grwpiau a fu'n rhan o'r gwaith datrys codau.
- Sgript neu graffig ar ffurf comig yn dangos holl wahanol gamau'r gwaith o ryng-gipio, dadgryptio a dadansoddi neges – ac yna sut mae modd defnyddio'r wybodaeth honno.
- Cyflwyniad mewn gwasanaeth neu sgwrs ar gyfer aelodau eraill eich grŵp ar bwysigrwydd defnyddio technoleg mewn rhyfel.

Gwaith Estynedig: Cynnal yr estyniad i weithgaredd 3 STEM – dolen.

Nawr, defnyddiwch rywfaint o'r wybodaeth rydych wedi'i chasglu i ddechrau ymchwilio i hanes lleol maes awyr milwrol yn eich ardal chi - gallwch wneud hyn gan ddechrau gyda'r map rhyngweithiol. Dros y ganrif ddiwethaf, defnyddiodd yr RAF 1,500 o safleoedd awyr neu leoliadau, felly hyd yn oes nad ydych chi'n byw ger un yn awr, byddai un wedi bod yn eich ardal chi ar ryw adeg.

Casglwch wybodaeth am y maes awyr. Pa wybodaeth neu ddealltwriaeth arall o gyfnod hanesyddol sydd eu hangen i adrodd stori'r maes awyr?

DATRYS CODAU

GWERSI I GEFNOGI'R CWRICWLWM A/NEU ARHOLIADAU

raf100schools.org.uk

CANLLAWIAU AR SUT Y GALLECH DDEFNYDDIO'R DEUNYDD HWN MEWN GWERS AM:

1. Yr Ail Ryfel Byd
2. Technoleg Rhyfela

Gellir defnyddio'r cwestiynau yn y bocs i archwilio'r thema hon a'r deunyddiau hefyd.

1. YR AIL RYFEL BYD

11–14 oed

Cwestiwn allweddol a awgrymir:

Pam oedd angen i'r datryswyr codau ddatblygu technoleg newydd i ddatrys codau byddin yr Almaen yn ystod yr Ail Ryfel Byd?

a) Dangoswch y ffilm berthnasol, *Codebreakers*, i'r myfyrwyr.

b) Gofalwch eu bod nhw'n gallu darllen y wybodaeth hanesyddol a'r bywgraffiadau a'r astudiaethau achos yn yr adran adnoddau.

c) Eglurwch i fyfyrwyr yn gweithio mewn grwpiau y byddant yn ceisio anfon negeseuon dirgel at ei gilydd ac y byddwch chi'n ceisio eu datrys nhw. Cyflwynwch seiffrau amnewid a rhowch enghraifft wedi'i chreu gan ddefnyddio cymal allweddol (e.e. yr enghraifft ROYAL AIR FORCE ar dudalen X). Rhannwch bob grŵp yn ddau a gofynnwch iddynt greu eu seiffr amnewid eu hunain ac ysgrifennu neges fer ac yna defnyddio'r seiffr i amgryptio'u neges. Dywedwch fod ganddyn nhw 15 munud i gwblhau'r ddwy ran o'r gweithgaredd.

   Gofynnwch i'r grwpiau gyfnewid eu henghreifftiau o'r negeseuon wedi'u hamgryptio (ond nid seiffrau). Gofynnwch iddyn nhw gadw'r wybodaeth yn gyfrinach rhagoch chi, a rhoi un darn o wybodaeth yn unig i chi - y llythyren sy'n codi fwyaf yn y neges (mae'n bosib y bydd mwy nag un).

   Gofynnwch i'r grwpiau gyfnewid seiffrau. Mae ganddyn nhw 10 munud i ddadgryptio'r neges.

   Eglurwch eich bod chi am geisio datrys eu seiffr. Dywedwch eich bod yn rhagweld mai'r llythyren maen nhw wedi'i nodi yw E (yn fwyaf tebygol). Sut hwyl gawsoch chi? Eglurwch y dadansoddiad amlder, a pham i chi ddewis cynyddu'ch tebygolrwydd o fod yn gywir drwy ddewis y llythyren E.

   There will be a raid at midday London time on the dockyards of Southampton. The keyword is Wintersun.

   Dangoswch y diagram o sut roedd Enigma'n gweithio iddynt.

ch) O'u profiad nhw o greu a thorri codau, gofynnwch i'r myfyrwyr sut wnaeth y peiriannau Enigma helpu'r Almaenwyr a sut iddyn nhw achosi problem i Brydain a'r Cynghreiriaid.

   Gofynnwch i'r disgyblion greu diagram o'r broses o greu seiffr ac amgryptio neges, ac yna'r broses o ryng-gipio a dadgryptio'r neges a defnyddio'r cynnwys. Gofynnwch iddyn nhw ddisgrifio pob cam a beth yw heriau'r cam hwnnw.

   Gofynnwch i'r myfyrwyr drafod sut wnaeth technoleg effeithio ar gyfathrebu yn ystod yr Ail Ryfel Byd, gan ddefnyddio enghreifftiau a phrofiadau maen nhw newydd gael blas arnynt.

   Yna gofynnwch i'r myfyrwyr ateb y cwestiwn:

   Pam oedd angen i'r datryswyr codau ddatblygu technoleg newydd i ddatrys codau byddin yr Almaen yn ystod yr Ail Ryfel Byd?

DATRYS CODAU

raf100schools.org.uk

2. TECHNOLEG RHYFELA

11–16 oed

Cwestiwn allweddol a awgrymir:

Beth mae'r gweithgareddau a wnaed yn Bletchley Park yn ei ddangos am rôl y tîm mathemateg a'r datryswyr codau yn y rhyfela yn ystod yr Ail Ryfel Byd?

a) Dangoswch y ffilm.

b) Rhowch gopi i bob myfyriwr o daflen waith estynedig STEM a'r templed dryswr (gweler isod).

Os ydych chi'n cynnal gweithgareddau RAF100 gydag athro gwyddoniaeth a bod y myfyrwyr wedi cwblhau'r gweithgaredd STEM eisoes, neu os nad ydych chi'n hyderus i wneud y gweithgaredd STEM, gallwch ddefnyddio'r gweithgaredd yn c) yn y wers enghreifftiol uchod.

c) I ategu'r gweithgaredd, a gan ddefnyddio'r wybodaeth a'r cynnwys hanesyddol yn y ffilm, gofynnwch i'r myfyrwyr greu map meddwl/diagram gwe o rôl cyfathrebu dirgel yn ystod rhyfel, gan wahaniaethu rhwng codau a seiffrau.

ch) Gofynnwch i'r myfyrwyr gyflwyno dadl yn cefnogi neu'n diystyru pwysigrwydd y rhai a oedd yn gweithio yn Bletchley Park yn ystod yr Ail Ryfel Byd.

Cloi: Pa mor bwysig oedd technoleg wrth wneud penderfyniadau yn ystod y Rhyfel?

Gwaith Estynedig: Ewch ati i ganfod sut mae seiffrau'n cael eu hanfon heddiw.

DATRYS CODAU

RAF 100

raf100schools.org.uk

Y GWEITHGAREDD STEM

Bydd pob myfyriwr angen copi o daflen Estyniad STEM 3 a thempled dryswr a phin hollti (neu bin bawd gyda chorcyn). I adeiladu'r dryswr, dylai myfyrwyr dorri o amgylch y **ddwy olwyn ar y Templed Dryswr a'u cysylltu drwy roi'r pin drwy ganol y ddwy, gweler y diagram isod...**

Dylent ddechrau drwy dorri'r amgryptiad ar gyfer y neges wedi'i rhyng-gipio a roddwyd (gweler y ffigur isod). 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.

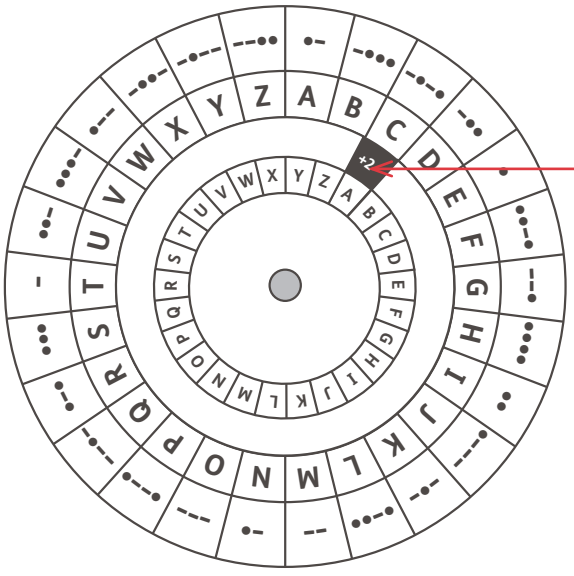
Yna dylai myfyrwyr roi cynnig ar ddadansoddiad amlder (o seiffr shift). Rhoddir neges fer wedi'i hamgryptio; dylent geisio datrys yr amgryptiad drwy ganfod pa lythyren sy'n cynrychioli E (gweler y ffigur isod). Yn olaf, dylent ddewis cymal a defnyddio'r dryswyr i'w amgryptio; gan gynyddu gosodiad y dryswr 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).

Y DRYSWR

Gall myfyrwyr greu dryswr drwy dorri'r ddwy olwyn ar eu Templed Dryswr.

Dylent ddechrau drwy osod y dryswr ar +2 a defnyddio'r gosodiad hwn i orffen amgryptio'r llythrennau "RAF" cyn rhoi cynnig ar eu geiriau a'u gosodiadau eu hunain.

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



DATRYS CODAU

raf100schools.org.uk

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 dirgel eu hunain (e.e. **+6**) cyn rhoi'r neges i'w partner i weld os gallan nhw dorri'r amgryptiad.

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 eu 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).

CWESTIYNAU YCHWANEGOL I GEFNOGI DYSGU AR GYFER POB GRŴP

- Pam oedd cynifer o fenywod yn cael eu cyflogi yn Bletchley Park?
- Pam mae angen diogelu rhai mathau o wybodaeth yn fwy nag eraill?
- Pwy oedd y gwyddonwyr/ mathemategwyr allweddol oedd yn gweithio yn Bletchley Park?
- Pam mae angen dadansoddi sawl darn o wybodaeth cyn gwneud penderfyniad i weithredu?
- Beth oedd rolau'r RAF a'r WRAF yn Bletchley Park ac mewn gwaith casglu cudd-wybodaeth mewn mannau eraill?

GWNEUD Y CYSYLLTIAD Â STEM

Nod y gweithgaredd STEM cysylltiedig yw dangos agwedd ar dechnoleg sy'n dangos sut roedd pobl yn meddwl yn y gorffennol. Yn y gweithgaredd STEM yma mae gofyn dylunio ac adeiladu cylched gyfathrebu. Gweithiwch gydag athro gwyddoniaeth i helpu myfyrwyr i archwilio sut mae modd anfon negeseuon dirgel fel signalau trydanol.