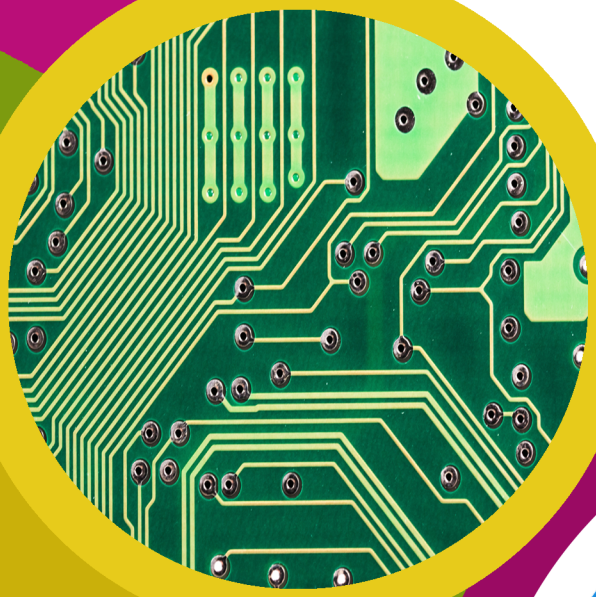
technocamps

Seiberddiogelwch Mewn Ysgolion Uwchradd



Llywodraeth Cymru
Welsh Government

Prifysgol Abertawe
Swansea University

Cardiff University
Prifysgol Caerdydd

Prifysgol Bangor University

Cardiff Metropolitan University
Prifysgol Metropolitan Caerdydd

University of South Wales
Prifysgol De Cymru

Cyngor Cyllido Addysg Uwch Cymru
Higher Education Funding Council for Wales
hefcw

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Prifysgol Aberystwyth University

Prifysgol Glyndŵr Wrecsam
Wrexham Glyndŵr University

institute of CODING in wales
technocamps

Trosolwg

Mae seiberddiogelwch yn angenrheidiol i ddiogelu ein data. Mae diogelu ein cyfrinair yn bwysig i bawb, gan fod pawb yn cael eu heffeithio gan dor-data, felly mae'n bwysig i ddysgwyr deall y pwysigrwydd o gael cyfrinair da.

Yn y gweithdy yma fyddwn ni'n dysgu sut i greu cyfrinair cryf, sut mae amgryptio'n gweithio, a sut mae hacwyr yn cracio cyfrineiriau a thorri mewn i systemau diogel.

Adnoddau Ar-Lein

Adnoddau Digidol:

https://tc1.me/educonf23resources

Amcan Dysgu?

- I ddeall pam mae cyfrineiriau cryf yn bwysig ac i fod yn hyderus mewn creu cyfrinair cryf.
- I ddeall ystyr y termau amgryptio a dadgryptio, yn benodol wrth sôn am God Morse a'r Seiffr Caesar.
- I ddeall y dulliau mae gwefannau yn defnyddio i geisio diogelu ein cyfrineiriau, ac i ddeall ni fydd hyn byth yn berffaith.

MDaPh Gwyddoniaeth a Thechnoleg

Cyfrifiaduraeth:

(CC4) Rwy'n gallu cynllunio a gweithredu strategaethau profi er mwyn adnabod gwallau mewn rhaglenni..

(CC4) Rwy'n gallu esbonio'r technegau a ddefnyddir i gadw a throsglwyddo data, a deall sut maen nhw'n agored i niwed.

(CC3) Rwy'n gallu esbonio pwysigrwydd diogelu'r dechnoleg rwy'n ei defnyddio a phwysigrwydd gwarchod safon fy nata.

(CC3) Rwy'n gallu esbonio sut mae fy nata yn cael eu defnyddio gan wasanaethau er mwyn fy helpu i wneud penderfyniadau mwy gwybodus wrth ddefnyddio technoleg.

(CC3) Rwy'n gallu esbonio sut mae data yn cael ei storio a'i brosesu.

Cysylltiadau i MDaPh Arall

Iechyd a Lles:

(CC4) Rwy'n gallu ystyried ffactorau perthnasol a goblygiadau wrth wneud penderfyniadau yn unigol ac ar y cyd.

(CC3) Rwy'n gallu adnabod ac asesu risg, a chymryd camau i'w leihau.

Y Pedwar Diben a Sgiliau Trawsgwricwlaidd

Mae'r adnodd hwn yn darparu cyfleoedd **Meddwl yn Feirniadol a Datrys Problemau**. Mae'n ofynnol i fyfyrwyr ddilyn cyfarwyddiadau a defnyddio'r wybodaeth darparwyd i ddadgodio ffeiliau llygredig a chreu algorithm gan ddefnyddio rhaglennu seiliedig ar flociau. Gallant ddadansoddi gwallau, nodi datrysiadau, a diddwytho'r camau nesaf.

Wrth drafod seiberddiogelwch a diogelwch ar-lein bydd dysgwyr gyda'r cyfle i ddatblygu eu **Heffeithlonrwydd Personol** trwy werthuso eu hymddygiad ar-lein a'u diogelwch, ac i ddefnyddio **Cynllunio a Threfnu** i ddatblygu strategaethau i ddiogelu eu hun ac eraill.

Mae'r adrannau **Rhyngweithio a Chydweithio** a **Data a Meddwl Cyfrifiadurol** y **FfCD** yn berthnasol i'r adnodd hwn. Bydd myfyrwyr yn dysgu sut i ddadansoddi'r problemau a gyflwynir iddynt, a chodio'n effeithlon gan ddefnyddio dewisiadau a digwyddiadau i greu algorithm. Bydd dysgwyr yn cydweithio i greu efelychydd gweinydd gyda'i micro:bit.

Pam Mae Dysgu Hyn yn Bwysig?

Mae'r adnodd hwn yn rhoi cyfle i ddysgwyr edrych ar bwysigrwydd diogelwch ar-lein a chyffredinolrwydd troseddau seiber. Byddant yn creu algorithmau syml gyda chymhwysiad amlwg, gan ddefnyddio iaith raglennu seiliedig ar flociau. Mae'n cyflwyno cysyniadau fel dewisiadau, dolennau, a rhaglennu seiliedig ar ddigwyddiadau sy'n hanfodol i'r ieithoedd rhaglennu mwyaf cyffredin. Mae'r adnodd hefyd yn dysgu pwysigrwydd cyfrineiriau cryf a ddiogel ac yn caniatáu ar gyfer gweithgareddau cydweithredol a rhyngweithiol i arddangos hyn. Gellir ehangu hyn i gyflwyno myfyrwyr i raglennu testun fel Python.

Allwedd Dulliau a Awgrymir

Yn y dull awgrymedig hwn rydym yn defnyddio'r lliwiau canlynol i wahaniaethu rhwng y mathau o weithgareddau:

- **Melyn - Esbonio.** Dylai athrawon esbonio'r sleid/enghraifft i'r dosbarth.
- **Gwyrdd - Trafod.** Dylai athrawon ddechrau trafodaeth agored gyda'r dosbarth i'w cael i roi adborth ar rai atebion/syniadau.
- **Porffor - Tasg.** Disgwylir i fyfyrwyr gwblhau gweithgaredd boed yn eu llyfrau gwaith neu ar y cyfrifiadur, ac yna trafodaeth am eu datrysiadau.
- **Gwyrdd - Cyflwyniad/Crynhoad.** Dylai athrawon ddosbarthu deunyddiau yn y cyflwyniad a gorffen y diwrnod gan gasglu deunyddiau ar y diwedd.

Cyflwyniad

Dechreuwch gyda chyflwyniadau, ac esboniad byr o raglen Technocamps, cyn dosbarthu unrhyw adnoddau sydd eu hangen ar ddysgwyr ac unrhyw gymhorthion ychwanegol ar gyfer dysgwyr ag anghenion ychwanegol.

Esboniad: Cynnwys y Sesiwn

Heddiw byddwn ni'n dysgu sut i fod yn ddiogel ar-lein trwy greu cyfrineiriau cryf. Erbyn diwedd y sesiwn byddwn ni'n deall sut mae cyfrineiriau yn cael ei gracio'n hawdd a'r pwysigrwydd o fod yn ddiogel.

Pam ydy Cyfrineiriau'n Bwysig?

Gofyn i'r dosbarth pam ydyn nhw'n meddwl fod cyfrineiriau'n bwysig:

- Maen nhw'n diogelu ein data
- Maen nhw'n diogelu ein hunaniaethau
- Maen nhw'n atal mynediad anawdurdodedig mewn i'n cyfrifon

Mae cyfrinair cryf a ddiogel yn lleihau'r risg o droseddwr seiber cyrchu ein data - oherwydd mae cyfrineiriau cymhleth a hir yn anoddach i ddyfalu neu gracio trwy ddulliau nerth bôn braich.

Yn ogystal, mae gan gyfrinair gwan y risg o ddatguddio'r hash ac yr algorithm hash (os mae'r cyfrinair wedi'i gracio) sy'n storio a diogelu'r cyfrinair - bydd hyn yn peryglu data pobl eraill hefyd.

Nodyn: Bydd esboniad o'r Hash nes ymlaen yn y gweithdy yma.

Mae Ymosodiadau Seiber yn Parhaus

Ewch i **tc1.me/threatmap** i weld ymosodiadau seiber yn digwydd yn fyw. Mae'r wefan yn amlinellu'r gwledydd a diwydiannau sydd wedi'i dargedu fwyaf a'r mathau o ddrwgwedd fwyaf poblogaidd (meddalwedd a ddefnyddir gyda bwriad maleisus i beryglu diogelwch cyfrifiadur).

Gadewch i'r dysgwyr archwilio'r wefan gan edrych ar y nodweddion gwahanol, megis dadansoddi yn ôl gwlad neu gynyddu cyfradd yr ymosodiadau.
Nodyn: Dyma'r bygythiadau sydd wedi'i dal, bydd bygythiadau llwyddiannus ddim yn dangos ar y wefan. A yw hyn yn peri pryder?

Ni Fydd yn Digwydd i Mi...

Esbonio i'r dysgwyr y camsyniad cyffredin fod pobl yn credu nad ydyn nhw mewn perygl o ymosodiad seiber, oherwydd ni fyddent yn darged.

Dangoswch (gyda'r wefan CyberThreat) bod mwyafrif o ymosodiadau yn digwydd yn erbyn gweinyddion a systemau mawr, nid unigolion. Sy'n golygu bod yr holl gyfrifon a chyfrineiriau datguddiwyd yn yr ymosodiad yn agored i niwed, a gall unrhyw un heb ei amddiffyn cael ei dal.

Have I Been Pwned?

Ewch i **tc1.me/pwned** i wirio a yw eich cyfeiriad e-bost wedi'i nodi mewn unrhyw dor-data yn y gorffennol. Rhowch gynnig ar sawl gyfeiriad e-bost, yn ddelfrydol cyfrifau personol a gwaith/ysgol (gan nad yw'n debygol fydd cyfeiriadau Hwb wedi'i effeithio).

Os ydych chi'n anlwcus ac mae gennych chi ddosbarth heb unrhyw dor-data, ceisiwch gydag e-bost ar hap - neu marl@gmail.com, sydd wedi'i ddal mewn 39 dor-data dros sawl wefan gan gynnwys datgeliad o'i ddinasyddiaeth Pwyleg - sy'n gwneud yn achos diddorol iawn!

Mae'n bwysig rydych chi'n ymwybodol fydd datgeliadau o wefannau pornograffig wedi'i rhestri hefyd. Enw'r wefan yn unig fydd yn ymddangos, ond mae'n werth sôn am hyn.

Nodyn: Mae'r nifer o gyfrifau "pwned" dros **12.5 biliwn!**

Pa Ddata All Gael ei Datgelu?

Cael trafodaeth fer gyda dysgwyr am ba ddata personol a gellir ei ddatgelu yn ystod hac?

Mae'r rhestr yma'n eang a bron yn ddiddiwedd, ond mae sawl esiampl ar y sleidiau. Ond yn y bôn gall unrhyw ddata sy'n cael ei storio ar-lein, yn gyhoeddus neu breifat, cael ei hacio a datgelu. Yn ogystal, mae'n bosib hacio unrhyw gyfrifiadur gyda chysylltiad i'r we.

...Felly Pam Poeni?

Cael trafodaeth fer am pam ddylem ni dal becso am ddiogelwch cyfrineiriau. Bydd y mwyafrif o wefannau (pob un dibynadwy) yn amgryptio'ch cyfrinair i'w storio, mae hyn yn golygu fod eich cyfrinair ond yn agored i niwed os yw'n syml iawn, os yw'r hash eisoes yn hysbys, neu os yw'n cynnwys digon o fanylion personol i'w ddyfalu.

Dangosir hyn ar y sleidiau ble mae'r ddau ddefnyddiwr a ddefnyddiwyd y cyfrinair "password" gyda'r un cyfrinair wedi'i amgryptio (hash). Mae hyn yn dweud wrth haciwr ar unwaith fod eich cyfrinair yn debygol i fod yn gyfrinair digon cyffredin i fwy nag un person ei ddefnyddio.

Wedyn fydd y haciwr yn chwilio am unrhyw gyfrinair hysbys (sydd wedi'i chracio'n flaenorol) a'u gyfrineiriau wedi'u hamgryptio, neu geisio gweithio allan ei hunain trwy ddyfalu'r cyfrinair (wedi gwneud yn haws trwy chwilio ar-lein gan ddefnyddio'r e-bost/enw ddefnyddiwr i ddarganfod gwybodaeth berthnasol am y defnyddiwr).

CyberChef

Ewch i **tc1.me/cyberchef**. Mae modd i'r wefan hon berfformio amgryptio, amgodio, cywasgu, a dadansoddi data. Bydd y gweithdy yma yn canolbwyntio ar ddangos **amgryptio** a rhywfaint o **ddadansoddi data**.

Am y dasg yma byddwn yn dangos sut rydym yn defnyddio "**hash**" fel dull o amgryptio cyfrineiriau. Ar ôl dewis ein dull amgryptio gallwn ni mewnbynnu unrhyw destun, clicio Bake, a gweld yr allbwn wedi'i amgryptio. Mae'r allbwn yma'n cyfateb i sut fydd cwmni yn storio ein cyfrineiriau yng nghronfa data, felly na all hyd yn oed y cwmni ddarllen eich cyfrinair.

Fodd bynnag, gellir gweld ychydig o bethau diddorol am y "hash":

- Bydd yr un llinyn mewnbwn bob amser yn cynhyrchu'r un llinyn allbwn - mae hyn yn golygu unwaith bydd y "hash" ar gyfer gyfrinair yn hysbys, bydd yn hysbys am byth.
- Nid oes unrhyw batrwm clir i'r amgryptio, bydd newidiadau bach yn y mewnbwn yn arwain at allbynnau hollol wahanol - felly mae'n anodd iawn i wrthdroi'r algorithm "hash", felly nid yw pob cyfrinair mewn perygl.
- Mae'r llinyn allbwn pob amser yr un hyd yn annibynnol o hyd y llinyn mewnbwn - mae yna fwy o fewnbynnau nag allbynnau felly mae'n bosib i gyfrineiriau rhannu "hash", gall cyfrinair syml cael yr un "hash" â chyfrinair cymhleth.

Bwysig: Trowch "**Autobake**" i ffwrdd (blwch ticio ar waelod y tudalen). Bydd hyn yn osgoi'r wefan chwalu mor aml. I ddod o hyd i'r amgryptiad MD5, teipiwch **MD5** mewn i'r bar chwilio ar y panel chwith (o dan y pennawd "**Operations**") neu scroliwch lawr i "**Hashing**". I ddefnyddio'r amgryptiad i'r mewnbwn llusgwch mewn i'r ardal "**Recipe**". Rhowch linyn mewnbwn o dan "**Input**" a chliciwch "**Bake**".

Yr "Hash" a MD5

Trafodwch fanteision defnyddio "hash" (mae hyn yn paru'n dda gyda'r gwybodaeth uchod ar yr hyn mae CyberChef yn ddangos) yn fyr gyda'r dysgwyr.

Pam mae MD5 wedi dyddio?

Mae MD5 yn cyfrifo'r hash yn gyflym iawn, roedd hyn yn fantais pan gafodd ei chreu. Fodd bynnag, oherwydd y cyflymder yma, gyda chymorth cyflymder cyfrifiaduron modern gallwch gyfrifo'r hash am lawer o gyfrineiriau posibl yn gyflym iawn i geisio torri i mewn i gyfrif rhywun.

Mae hyn hefyd yn golygu ei bod hi'n hawdd iawn creu tablau o gyfrineiriau a'u hash, gan wneud hi'n llawer haws i chi a hacwyr y dyfodol ddod o hyd i'r cyfuniad cyfrinair/hash cywir yn gyflymach. Dyma reswm arall y dylai eich cyfrinair fod yn anodd ei ddyfalu.

Dyfalu Hash

Dangoswch hash o gyfrinair syml i'r dysgwyr a gofynnwch iddyn nhw ddefnyddio CyberChef i geisio paru'r hash mor gyflym ag y gallant, a thrwy hynny ddod o hyd i'r cyfrinair cywir.
Er enghraifft yr hash: **5f4dcc3b5aa765d61d8327deb882cf99**
Am y cyfrinair: **password**

Naill ai defnyddiwch yr enghraifft hon neu meddyliwch am fwy i annog dysgwyr i geisio dod o hyd i'r cyfrinair cywir gyflymaf, gan ddangos y symlrwydd torri i mewn i gyfrif gyda'r dull hwn.

Datgeliadau Cyfrinair Osgoadwy ac Anosgoadwy

Trafodwch gyda'r dysgwyr y rhesymeg y tu ôl i ddatgeliadau cyfrinair sy'n bosib osgoi neu amhosib osgoi - ni allwch reoli bod rhywun yn eich hacio, ond gallwch osgoi:

- Rhoi gwybodaeth bersonol i bobl
- Ysgrifennu cyfrineiriau rhywle hawdd eu darganfod
- Rhywun yn gweld eich cyfrinair
- Defnyddio gwybodaeth bersonol yn eich cyfrinair

Er bod rhyng-gipio eich cyfrinair a chael eich bysell-logio y tu hwnt i'ch rheolaeth, ar y cyfan bydd cyfrinair cryf yn dal i gael ei ddiogelu rhag ymosodiadau nerth bôn braich, neu rywun sy'n chwilio am hash cyfrinair sydd wedi'i storio yn y rhwydwaith.

Beth Sy'n Gwneud Cyfrinair Diogel?

Trafod cyflwr cyfrineiriau yn y DU, gyda'r mwyafrif o bobl yn dal i ddefnyddio cyfrineiriau anniogel – naill ai drwy gynnwys gwybodaeth bersonol (sy'n bosib darganfod yn hawdd o chwiliad ar rwydweithiau cymdeithasol) neu drwy ddefnyddio cyfrineiriau hynod gyffredin.

Trafodwch beth sy'n gwneud cyfrinair cryf:

- Beth ddylai ei gynnwys?
- Beth na ddylai ei gynnwys?

Beth Sy'n Gwneud Cyfrinair Diogel?

Eglurwch i'r dysgwyr, er bod yr elfennau cyffredin a ddyfynnir mewn cyfrinair diogel (llythrennau mawr a bach, rhifau a symbolau) i gyd yn bwysig, y ffactor pwysicaf yw hyd.

Mae cyfrifiaduron yn dda iawn am gyflawni tasgau'n gyflym, a'r prif ffactor wrth atal cyfrifiadur rhag cracio'ch cyfrinair yw ei gwneud hi'n ddigon hir fel nad yw'r cyfrifiadur byth yn debygol o'i gael yn iawn.

Nodyn: Mae hyn tua 16 nod o hyd.

Cyfrineiriau Diogel

Gofynnwch i'r dysgwyr fynd i **tc1.me/nordpass** i wirio pa mor ddiogel yw eu cyfrineiriau.

Dechreuwch trwy roi cynnig ar y ddwy enghraifft ar y sleid i ddangos y gwahaniaeth rhwng y cyfrinair sy'n ymddangos yn gymhleth a'r cyfrinair syml ond hirach.
Yna gofynnwch i'r dysgwyr roi cynnig ar eu cyfrineiriau eu hunain i wirio pa mor ddiogel maen nhw wedi bod!

Sut i Aros yn Ddiogel

Nawr rydyn ni'n gwybod bod un cyfrinair hir, hawdd i'w gofio yn llawer mwy diogel na chyfrinair byr, cymhleth iawn. Fodd bynnag, mae gan nifer o wefannau ofynion llym o ran yr hyn y mae'n rhaid i'ch cyfrinair ei gynnwys!

Defnyddiwch Reolwr Cyfrinair!

Mae gan lawer o bobl amheuon ynghylch rheolwyr cyfrinair gan eu bod yn storio eu holl fesurau diogelwch mewn un lle. Fodd bynnag, mae'r gwefannau hyn yn tueddu cael mesurau diogelwch da iawn eu hunain, ac rydym bellach yn gwybod sut i wneud cyfrinair diogel ein hunain.

Bydd rheolwyr cyfrinair yn creu ac yn storio cyfrineiriau cymhleth a diogel ar gyfer pob gwefan ble mae gennych chi gyfrif. Mae hyn yn golygu mai dim ond un cyfrinair hir, hawdd ei gofio a ddiogel y bydd ei angen arnoch, ond bydd gennych chi gyfrineiriau hir, cymhleth ac unigryw o hyd i bob un o'ch cyfrifon a all basio gofynion pob gwefan.

Fforensig Digidol

Cyflwyno'r cysyniad o Fforensig Digidol a pham ei fod yn set sgiliau pwysig i'r heddlu a chwmnïau diogelwch ei chael. Fodd bynnag, fel gydag unrhyw beth, gall y wybodaeth hon gael ei chamddefnyddio, a'r un arfau sy'n ei gwneud yn bosibl dod o hyd i droseddwyr yw'r arfau y maent wedi'u defnyddio i gyflawni'r drosedd.

Yna cyflwynwch y dasg sy'n ofynnol gan y dosbarth.

Ffon Gof

Ewch i **tc1.me/MemoryStick** a naill ai pwyswch y botwm llwytho i lawr yng nghornel dde uchaf y dudalen i lawrlwytho ffeil zip, neu lawrlwythwch bob un o'r ffeiliau yn unigol.

Cyn eu llusgo i mewn i adran fewnbwn CyberChef (**tc1.me/cyberchef**). Trafodwch y ffeiliau y maent wedi'u llwytho i lawr, nid oes unrhyw fath o ffeil nac eicon adnabyddadwy, wrth eu hagor maent yn ymddangos yn ffregod.

Llusgwch nhw i CyberChef, bydd un yn cael ei adnabod ar unwaith fel delwedd.

Unwaith eto gwnewch yn siŵr bod "Autobake" wedi'i **diffodd**.

Steganograffeg

Cyflwynwch y cysyniad o steganograffeg i'r dysgwyr a'r gwahanol ddulliau y gellir ei ddefnyddio.

Cyfarwyddwch nhw i edrych ar y tab Fforensig ar CyberChef i weld a ydyn nhw'n gallu adfer unrhyw wybodaeth o'r ddelwedd.

Steganograffeg

Mae yna wybodaeth wedi'i chuddio tu mewn i'r ddelwedd, i ddod o hyd i hyn ar CyberChef defnyddiwch un o'r gweithrediadau fforensig canlynol:

- **Randomize Colour Palette**
- **View Bit Plane**

Mae "Randomize" yn rhoi lliw ar hap i bob lliw yn y ddelwedd - mae hyn yn golygu bod gwybodaeth sydd wedi'i chuddio mewn golwg blaen trwy gael lliw ychydig yn wahanol i'r picseli cyfagos yn cael ei gwneud yn glir.

Mae "View Bit Plane" yn debyg i sut mae steganograffeg Bit Lleiaf Arwyddocaol yn gweithio - mae gwerth deuaidd pob picsel yn cael ei rannu dros sawl delwedd du a gwyn gwahanol. Mae hyn yn golygu bod yr hyn a oedd yn wahaniaeth bychan iawn yn y ddelwedd wreiddiol yn sydyn yn wahaniaeth mawr yn y "Bit Plane".

Mae'r testun a ddatgelwyd yn dweud wrthym fod y ffeil "temp" wedi'i amgryptio â Chod Morse a Seiffr Caesar.

Cod Morse

Mae cod Morse yn system gyfathrebu sy'n defnyddio toriadau a dotiau i gynrychioli llythrennau.
Mae hyn yn caniatáu i chi guddio eich neges trwy newid y llythrennau i'w toriadau a dotiau cyfatebol. Mae hwn yn debyg i seiffr amnewid, fel Seiffr Caesar.

Seiffr Caesar

Dull o amgryptio yw Seiffr Caesar, sy'n newid pob llythyren o'r testun plaen gan syfliad penodol o'r wyddor e.e. byddai'r testun plaen "ABCDE" gyda syfliad o werth 2 yn amgodio i "CDEFG".

I ddefnyddio olwyn Seiffr Caesar, rydych chi'n cylchdroi'r olwyn allanol fel bod yr "A" allanol yn cyd-fynd â'r rhif syfliad ar y cylch mewnol.
I amgryptio, y neges rydych chi'n ei darllen o'r tu allan i mewn ac i'w dadgryptio, rydych chi'n darllen o'r tu fewn allan.

Ewch i **tc1.me/CaeserCipher** i weld hyn ar waith.

Cod Morse a Seiffr Caeser

Yn CyberChef, ar y ffeil "**temp**", llusgwch y gweithrediad **From Morse Code** i'r rysáit a chliciwch "Bake". Bydd hyn yn newid cynnwys y ffeil i'r hyn sydd amlwg yn eiriau ond yn parhau i gael syfliad Caeser.

Ychwanegwch y gweithrediad **ROT13** (Seiffr Caeser) yn y rysáit a chliciwch "Bake". Bydd angen profi pob un o'r 25 syfliad i ddod o hyd i'r un cywir. Yn lle hynny gallwn lusgo gweithrediad **ROT13 Brute Force** i ddangos bob syfliad ar unwaith!

Nodyn: Gwerth y syfliad cywir yw **19**.

Mae hyn yn rhoi ein hamgryptiad ffeil terfynol i ni (**RC4**) a'i "passphrase" (**T3CHN0C4MPS!**)

RC4

Mae RC4 yn ddull darfodedig o amgryptio, fodd bynnag, gellir ei ddefnyddio o hyd i ddeall egwyddorion amgryptio.

Llusgwch **RC4** i'r adran Recipe, a theipiwch y cyfrinair (**T3CHN0C4MPS!**).

Agorwch y ffeil "**bin**" a chliciwch "Bake". Dylai hyn wedyn agor rhestr o gyfrineiriau i gyfrifon ffug Hwb.

Cyflwyno'r micro:bit

Os nad oes gan y dosbarth unrhyw brofiad gyda'r micro:bit gyflynwch y dyfais!

Mae'r micro:bit yn gyfrifiadur bychan a adeiladwyd gan bartneriaeth rhwng y BBC a Microsoft, a grëwyd gyda'r bwriad o ysbrydoli pobl ifanc i godio ac arddangos sut mae caledwedd a meddalwedd yn gweithio gyda'i gilydd.

Mae'r micro:bit yn llawn synwyryddion gwahanol sy'n eich galluogi ni i greu nifer fawr o raglenni a syniadau. Mae'r rhain i gyd ar y sleidiau cysylltiedig.

Gwiriwr Cyfrinair micro:bit

Eglurwch i'r dysgwyr ein bod ni'n mynd i geisio gwneud gwiriwr cyfrinair gyda micro:bit!

Bydd hyn yn efelychu mewngofnodi i wefan, lle mae un micro:bit yn gweithredu fel y ddyfais sy'n ceisio mewngofnodi, a'r llall yn ymddwyn fel gweinydd y wefan yn gwirio'r cyfrinair.

Yn gyntaf, byddwn yn rhaglennu'r gweinydd, ond gellir rhaglennu'r ddau micro:bit gyda'r ddwy ran os dymunwch.

Gweinydd micro:bit

Dilynwch y cod a ddarperir yn y sleidiau i godio'r Gweinydd microbit.

Mae hwn yn mynd i weithredu fel gweinydd gwefan, gan storio eich manylion mewngofnodi fel bod pan fyddwch yn ceisio mewngofnodi gyda microbit arall bydd y gweinydd yn gwirio'r enw defnyddiwr a chyfrinair a roddwch yn erbyn ei gofnodion i ganiatáu i chi mewngofnodi.

Yn y sefyllfa hon mae'r grŵp radio a ddefnyddiwch yn gweithredu fel cyfeiriad IP gwefan, gan sicrhau eich bod chi wedi cysylltu â'r wefan gywir pan fyddwch yn darparu eich manylion mewngofnodi.

Gellir adeiladu hyn ar un microbit neu'r ddau. Mae'n gwneud mwy o synnwyr gydag un, ond dyma'r darn hirach o god felly os byddai'n well gennych osgoi un dysgwr yn gwneud mwy nag un arall, mae hynny'n bosibl.

Dyfais micro:bit

Dilynwch y cod a ddarperir yn y sleidiau i godio'r Ddyfais microbit.

Mae hwn yn mynd i weithredu fel eich dyfais bersonol, yn cysylltu â'r cyfeiriad IP cywir gwefan ac yn ceisio mewngofnodi gyda'ch enw defnyddiwr a chyfrinair. Os yw eich manylion yn cyfateb yna bydd y wefan yn mewngofnodi chi ac yn darparu ymateb.

Gellir adeiladu hyn ar un microbit neu'r ddau.

Estyniadau micro:bit

Gallu anfon negeseuon i'r micro:bit (fel pe bai'n postio sylw i'r wefan) lle mae'n rhaid i'r micro:bit wirio yn gyntaf a ydych wedi mewngofnodi. Gallwch wneud hyn trwy wneud newidyn o'r enw **LoggedIn** sydd fel arfer wedi'i osod i **Gau** ond wrth fewngofnodi daw'n **Wir**. Defnyddiwch flociau **anfon** a **derbyn tesun** yn lle'r blociau **gwerth** a gwiriwch a yw'r defnyddiwr wedi mewngofnodi cyn dangos y neges.

Ychwanegu dull o amgryptio fel nad yw'r 'gweinydd' yn storio cyfrinair testun plaen. Gallwch wneud hyn trwy wneud y cyfrinair yn rhif a gwneud **gweithrediadau mathemategol** arno (e.e. sin). Nid yw hyn yn wir amgryptio ond mae'r cysyniad yr un peth. Storiwch eich cyfrinair fel y gwerth wedi'i amgryptio a pherfformiwch y gweithrediad ar y **gwerth a dderbyniwyd**.

Ychwanegwch restr o enwau defnyddwyr a chyfrineiriau sydd â chaniaâd mewngofnodi i'r micro:bit. Gallwch wneud hyn trwy ddefnyddio **rhestr (arae)** yn lle **newidyn** i storio'r enwau defnyddwyr a'r cyfrineiriau. Bydd angen i chi wirio **lleoliad** un i sicrhau eich bod yn gwirio'r cyfrinair cywir ar gyfer yr enw defnyddiwr cywir.

Estyniad - How To Rob A Bank

Mae hwn yn weithgaredd tywys llawn hwyl a ddatblygwyd gan CyberSkills.

Bydd y dysgwyr yn cael eu harwain trwy ddefnyddio gorchmynion terfynell i gyrchu a chwilio trwy system fancio am wybodaeth cyfrif. Yna byddant yn defnyddio'r wybodaeth honno i drosglwyddo arian allan o gyfrifon pobl.