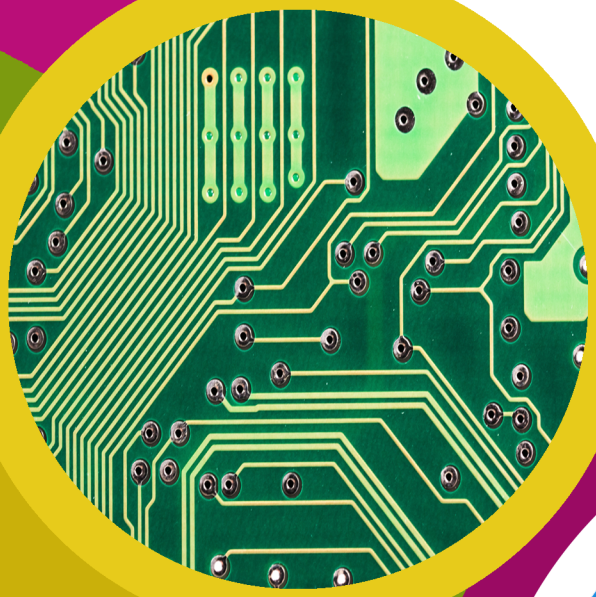
technocamps

Cryptograffeg
Canllaw Athrawon



UNDEB EWROPEAIDD EUROPEAN UNION
Llywodraeth Cymru Welsh Government
Cronfa Gymdeithasol Ewrop
European Social Fund

Prifysgol Abertawe Swansea University
CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD
PRIFYSGOL BANGOR UNIVERSITY
Cardiff Metropolitan University
Prifysgol Metropolitan Caerdydd
i.t.wales
PRIFYSGOL ABERYSTWYTH UNIVERSITY
PRIFYSGOL glyndŵr Wrecsam
Wrexham glyndŵr UNIVERSITY
University of South Wales Prifysgol De Cymru

MDaPh Gwyddoniaeth a Thechnoleg

Cyfrifiaduraeth:

(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.

Bod yn Chwilfrydig:

(CC4) Rwy'n gallu disgrifio effeithiau gwyddoniaeth a thechnoleg, y gorffennol a'r presennol, ar gymdeithas.
(CC3) Rwy'n gallu gwerthuso dulliau er mwyn awgrymu gwelliannau.

MDaPh Eraill

Dyniaethau:

(CC3) Rwy'n deall sut mae ffactorau yn y gorffennol a'r presennol wedi siapio fy nghymunedau.

Y Pedwar Diben a Sgiliau Trawsgwricwlaidd

Mae'r adnodd hwn yn darparu cyfleoedd ar gyfer **Meddwl yn Feirniadol a Datrys Problemau** drwyddo draw. Wrth werthuso pob dull amgodio ac amgryptio, bydd y dysgwyr yn adnabod problemau posibl gyda diogelwch y dulliau ac yn gallu awgrymu ffyrdd o wella arnynt.

Ymdrinnir â rhai o agweddau sylfaenol llinyn **Data a Meddwl Cyfrifiadurol** y **FfCD** yn yr adnodd ac mae angen i ddysgwyr ddilyn cyfarwyddiadau dadgryptio er mwyn derbyn y negeseuon testun plaen. Bydd unrhyw gamgymeriadau a wnânt yn ystod y broses ddadgryptio yn rhoi'r cyfle iddynt gywiro'r camgymeriadau y maent wedi'u gwneud.

Pam Mae Dysgu Hyn yn Bwysig?

Mae'r adnodd hwn yn galluogi'r dysgwyr i archwilio hanes cryptograffeg a dysgu'r ffyrdd sylfaenol y mae gwybodaeth wedi'i cyfathrebu'n gyfrinachol ers milenia. Archwilir datblygiadau gwahanol dechnegau amgodio ac amgryptio a gall dysgwyr gymhwyso'r technegau i gael mynediad at wybodaeth sydd wedi'i chuddio mewn cod. Mae cryptograffeg yn chwarae rhan fawr mewn amddiffyn pobl ar-lein, boed hynny wrth ddiogelu eu manylion dilysu ar gyfer gwefan, neu gadw eu negeseuon personol at ffrindiau a theulu yn breifat. Mae'r adnodd hwn yn gyflwyniad i fyd seiberddiogelwch a phwysigrwydd cadw'n ddiogel ar-lein.

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 ddysgwyr 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, cyn dosbarthu unrhyw adnoddau a sydd angen ar bob dysgwr ac unrhyw gymorth i helpu dysgwyr gydag anghenion dysgu ychwanegol.

Tasg: Cynllun Corryn

Dysgwyr i lenwi'r diagram pry cop gydag enghreifftiau o bryd y maent yn meddwl bod angen iddynt anfon a derbyn negeseuon diogel.

Esbonio: Steganograffeg

Steganograffeg yw'r arfer o guddio negeseuon neu wybodaeth o fewn testun neu ddata nad ydynt yn gyfrinachol.

Daw Steganography o'r Groeg steganos sy'n golygu cudd a graphein yn golygu ysgrifennu.
Defnyddir steganograffeg mewn dyfrnodi digidol ac weithiau fe'i defnyddir i anfon negeseuon cudd.

Mae enghraifft yn cynnwys:
- Dyfrnodi
- Inc aweledig
- Seiffrau Bacon
- Micro-smotiau

Tasg: Diffinio Steganograffeg

Dysgwyr i lenwi adrannau llyfr gwaith ar:
- Beth yw steganograffeg?
- Beth mae steganograffeg yn ei olygu?
- Pryd mae steganograffeg yn cael ei ddefnyddio?

Esbonio: Gwas Histiaeus

Anfonodd Histiaeus neges at ei fasal trwy eillio pen ei was mwyaf dibynadwy, yna tatŵio'r neges ar gefn pen y gwas. Ar ôl i wallt y gwas dyfu'n ôl, anfonodd Histiaeus y gwas i ffwrdd at y fassal. Pan gyrhaeddodd y gwas, fe eillio ei ben i ddatgelu'r neges gudd.

Mae hwn yn fath o steganograffeg. Pe chwilid y gwas, ni ddeuid o hyd i neges oni bai iddynt eillio ei ben.

Tasg: Gwas Histiaeus

Dysgwyr i dynnu llun bwrdd stori o esiampl y gwas yn eu llyfrau gwaith.

Trafod: Problemau gyda'r System

Trafodwch gyda'r dosbarth pa broblemau sydd yn ein hesiampl gwas:

Pa mor hir mae'n ei gymryd i anfon neges?
Mae'n rhaid i ni eillio'r pen, tatŵio'r pen ac yna aros am amser hir i'r gwallt dyfu'n ôl. Felly nid yw'n bosibl anfon neges yn gyflym.

A ellir defnyddio'r un system a gwas sawl gwaith?
Gellid defnyddio'r system sawl gwaith, ond nid yw tatŵs yn dod i ffwrdd yn union, felly efallai y bydd angen gwas gwahanol bob tro.

Ydym ni'n cael berchen ar weision a thatŵio nhw?
Na, nid oes gennym weision mwyach ac mae pobl yn annhebygol o gydsynio i ni datŵio negeseuon cyffredinol ar eu pennau.

Esbonio: Syr Francis Bacon

Ganed Syr Francis Bacon yn 1561 a bu farw yn 1626. Gwasanaethodd fel cynghorydd cyfreithiol i'r Frenhines Elisabeth. Pan olynodd y Brenin Iago I y Frenhines Elizabeth, tyfodd safle Francis Bacon yn gyflym iawn. Gwnaethpwyd ef yn farchog, yna gwnaed ef yn Farwn, ac o'r diwedd rhoddwyd y teitl Is-iarll St. Alban.

Mae Francis Bacon wedi'i alw'n dad empirigiaeth, y dylai gwybodaeth wyddonol fod yn seiliedig ar ymresymu ac arsylwadau anwythol yn unig. Cyn hyn, roedd pobl yn dilyn y dull Aristotleaidd: Pe bai dynion digon deallus yn trafod pwnc yn ddigon hir, byddent yn darganfod y gwir.

O ganlyniad mae Francis Bacon yn aml yn cael ei gredydu fel tad y dull gwyddonol.

Yn bwysig i ni, fe luniodd ddull steganograffig o guddio negeseuon trwy ddefnyddio gwahanol ffontiau.

Esbonio: Y Seiffer Bacon

Mae'r seiffr Bacon yn ddull o guddio neges y tu mewn i neges arall trwy newid y ffont.

Y cam cyntaf yw ysgrifennu ein neges gudd. Yna byddwn yn dewis dau fath gwahanol o ffont megis print trwm ac italig neu sans comic a sgript Edwardaidd.
Yna rydyn ni'n ysgrifennu neges ddiflas sydd angen o leiaf 5 gwaith cymaint o lythrennau ynddi â'n neges gudd.
Un o'n ffontiau fydd A, un fydd B. Rydym yn newid ffont ein neges ddiflas o A i B ar gyfer pob llythyren gyfatebol yn ein neges gudd.

Nawr ewch drwy'r enghraifft yn y sleidiau gam wrth gam fel bod y dysgwyr yn deall yn iawn sut mae'r broses amgodio yn gweithio.

a: AAAAA	h: AABBB	o: ABBBA	v: BABAB
b: AAAAB	i: ABAAA	p: ABBBB	w: BABBA
c: AAABA	j: ABAAB	q: BAAAA	x: BABBB
d: AAABB	k: ABABA	r: BAAAB	y: BBAAA
e: AABAA	l: ABABB	s: BAABA	z: BBAAB
f: AABAB	m: ABBAA	t: BAABB	
g: AABBA	n: ABBAB	u: BABAA	

Tasg: Ymarfer Seiffr Bacon

Dysgwyr i geisio dadgryptio'r negeseuon a ddarperir ar y sleidiau ac yn eu llyfrau gwaith.

Datrysiadau:

Yr aMSEr yw CHWEcH O'R gloch YN SIapAn
ABBAA ABBBA AAABA AABBB BBAAA ABBAB
M O C H Y N

YDY mAE LLAEtH Yn fLAsus
AAABA AAAAA BAABB AABBB
C A T H

RHEDeg Yn hWyR EtO
AAAAB BABBA BAABA
B W S

yDych Chi'n DIGOn DDEwr i Roi GyNnig AR YR uN HON NEU ydY Hl'n eich OFnl?
BABBB ABBBA AAABA AABBB ABBAB ABBBA AAABA AAAAA ABBAA ABBBB BAABA
T E C H N O C A M
P S

Trafod: Problemau gyda'r Seiffr Bacon

Trafodwch gyda'r dosbarth pa broblemau sydd yn y Seiffr Bacon:

Pa mor amlwg yw hi bod rhywbeth wedi'i guddio yn y neges?

Mae'n amlwg iawn bod rhywfaint o neges wedi'i chuddio yn y testun oherwydd nid yw ffontiau gwahanol yn gynnil iawn. Po agosaf yw'r dewis o ddau ffont at ei gilydd, y lleiaf amlwg yw bod neges gudd ond bydd hyn yn ychwanegu at yr anhawster o amgodio a dadgodio'r neges.

Pa mor anodd fyddai gwneud hyn â llaw?

Datblygwyd y dull hwn yn y 1600au felly byddai'r rhan fwyaf os nad pob neges wedi'u hysgrifennu â llaw. Mae creu dau ffont gwahanol a chyfnewid rhyngddynt wrth ysgrifennu â llaw yn eithaf anodd yn enwedig pan fo angen i nodau fod yn gyson.

Estyniad: Creu Inc Anweledig eich Hun

Dysgwyr i gymysgu un rhan soda pobi ag un rhan o ddŵr. Gan ddefnyddio blagur clust, ysgrifennwch neges ar ddarn o bapur ar wahân.

Arhoswch i'r inc anweledig sychu.

Paentiwch yn ysgafn dros y papur "plaen" gyda sudd ffrwythau tywyll.

Dylid datgelu'r neges gudd.

Dylai dysgwyr wedyn ysgrifennu'r camau ar gyfer gwneud yr inc yn eu llyfrau gwaith.

Gofynnwch a oes gan y dysgwyr syniad pam mae hyn yn digwydd: Adwaith Asid + Alcali yn achosi newid lliw ar y papur.

Trafod: Ail-Ymweld

Ailadroddwch y technegau steganograffig y mae'r dysgwyr wedi'u defnyddio, sut maen nhw'n gweithio a'r problemau sy'n gysylltiedig â nhw.

Tasg: Beth yw Cryptograffeg?

Dysgwyr i ysgrifennu beth maen nhw'n meddwl yw cryptograffeg yn eu llyfrau gwaith.

Esbonio: Cryptograffeg

Cryptograffeg yw ymarfer ac astudio technegau a ddefnyddir ar gyfer cyfathrebu diogel.

Daw cryptograffeg o'r Groeg kryptos sy'n golygu cyfrinach a graphein yn golygu ysgrifennu.

Defnyddir technegau cryptograffig drwy'r amser ym mywyd beunyddiol heb i chi hyd yn oed sylwi. Mae enghreifftiau yn cynnwys:

- Taliadau cyfrif banc
- Pori gwe
- Apiau negeseuon gan gynnwys Snapchat a WhatsApp
- Siopau ar-lein a dilysu cyfrifon defnyddwyr

Mae cryptograffeg yn wahanol i steganograffeg. Nid ydym yn cuddio'r ffaith bod neges wedi'i hanfon. Yn lle hynny mae ein diogelwch yn deillio o'r anhawster i ddadgryptio'r neges heb allwedd benodol sydd wedi'i defnyddio wrth amgryptio.

Activity: Diffinio Cryptograffeg

Dylai dysgwyr lenwi eu llyfr gwaith:

- Beth yw cryptograffeg?
- Beth mae cryptograffeg yn ei olygu?
- Pryd mae cryptograffeg yn cael ei ddefnyddio?
- Sut mae cryptograffeg a steganograffeg yn wahanol?

Esbonio: Codlyfrau

Mae un dull cryptograffig a ddefnyddir yn gyffredin yn seiliedig ar lyfrau cod. Rydym yn ysgrifennu llyfr unfath a geiriadur cyfan sy'n newid ystyr geiriau neu ymadroddion.

Mae gennym gopi ac mae gan y derbynnydd gopi.
Rydyn ni'n ysgrifennu ein neges ac yn amgryptio pob gair o ymadrodd yn y neges yn ôl ein codlyfrau.

Mae ein derbynnydd yn dadgryptio'r neges gan ddefnyddio copi union yr un fath o'r codlyfr.

Tasg: Creu Codlyfr eich Hun

Dylai dysgwyr gwblhau'r gweithgaredd yn eu llyfrau gwaith ar greu eu codlyfrau eu hunain.
Gofynnwch i rai dysgwyr rannu eu negeseuon, yn enwedig y rhai sydd wedi rhoi cynnig ar yr estyniad.

Trafod: Siaradwyr Cod

Mae newid geiriau ac ymadroddion unigol yn ystod amgryptio yn debyg i gyfieithu i iaith arall y gobeithiwn nad yw clustfwr (eavesdropper) yn ei siarad. Mae'r math o godlyfr yn gweithio fel llyfr ymadroddion neu eiriadur ar gyfer ail iaith

Mae angen i ni wneud yn siŵr nad yw'r iaith rydyn ni'n dewis amgryptio iddi yn cael ei siarad yn eang. Allwn ni feddwl am unrhyw ieithoedd anhysbys?

Mae'r Gymraeg yn iaith weddol anhysbys ac wedi cael ei defnyddio mewn gwirionedd yn ystod rhai rhyfeloedd fel techneg amgryptio. Mae hyn oherwydd nad oes llawer o bobl y tu allan i Gymru yn siarad Cymraeg.

Esbonio: Siaradwyr Cod Navajo

Yn ystod yr ail ryfel byd, defnyddiodd yr Americanwyr Navajo brodorol America fel siaradwyr cod. Ychydig iawn o bobl y tu allan i'r ardaloedd Navajo oedd yn siarad yr iaith Navajo.

Felly roedd cyfieithu'r negeseuon milwrol i Navajo cyn eu hanfon dros y radio yn system amgryptio wych. Byddai gan bob platŵn berson Navajo a oedd yn gyfrifol am amgryptio a dadgryptio negeseuon.

Defnyddiwyd hwn amlaf yn y brwydrau o amgylch De'r Môr Tawel. Os nad oedd pobl yn America y tu allan i'r ardaloedd Navajo yn siarad yr iaith yna roedd yn annhebygol iawn y gallai'r Japaneaid ei deall.

Fodd bynnag, roedd rhai problemau diddorol gyda defnyddio Navajo. Nid oedd gan dermau milwrol modern yn Saesneg yr un peth yn Navajo, felly cafodd cychod eu henwi ar ôl creaduriaid y môr, tra bod awyrennau a hofrenyddion yn cael eu henwi ar ôl adar.

Esbonio: Seiffr Pig Pen

Mae Seiffr Pig Pen wedi cael ei ddefnyddio drwy gydol hanes fel techneg amgryptio gan grŵp cyfrinachol o'r enw'r Seiri Rhyddion.

Mae'r Seiri Rhyddion yn sefydliad brawdol sy'n debyg i glwb cyfrinachol. Mae ganddyn nhw ysgwyd llaw, codau a defodau arbennig nad ydyn nhw i fod i'w rhannu â'r byd y tu allan.

Hefyd ni chaniateir iddynt ysgrifennu unrhyw un o'u defodau cychwyn mewn Saesneg clir. Mae cymaint o aelodau newydd yn defnyddio seiffrau fel y seiffr pig pen i gofnodi'r rheolau i'w gwneud yn haws iddynt ddysgu.

I ddefnyddio'r seiffr pig pen, mae pob llythyren yn eich neges testun plaen yn cael ei hamgryptio gan ddefnyddio'r grid a welir yn llyfrau gwaith y dysgwyr.

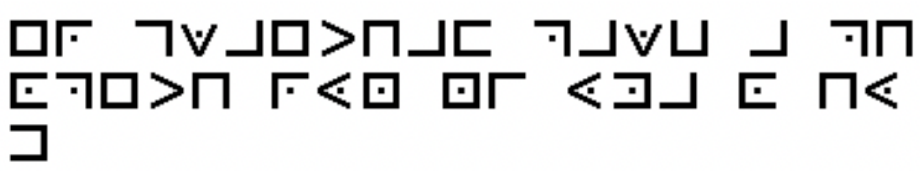
Yna mae'r symbolau rhyfedd yn cael eu hanfon fel y neges a'r derbynnydd yn eu dadgryptio.

Tasg: Ymarfer Pig Pen

Dylai dysgwyr geisio amgryptio a dadgryptio'r negeseuon a ddarperir yn eu llyfrau gwaith.
Datrysiadau:

Hei Mister Urdd:

Er gwaethaf pawb a phopeth ry'n ni yma o hyd:



Aderyn Melyn I fyny yn y goeden Banana

Nid wy'n gofyn bywyd moethus aur y byd na'i berlau man.

Trafod: Codes vs. Seiffrau

Trafodwch gyda'r dosbarth y gwahaniaethau rhwng codau a seiffrau:

- Sut mae seiffr pig pen yn wahanol i lyfr cod?
- Beth mae llyfr codau yn ei amgryptio?
- Beth mae seiffr pig pen yn ei amgryptio?
- Felly beth yw'r gwahaniaeth rhwng cod a seiffr?

Mae seiffr pig pen yn amgryptio llythrennau unigol tra bod llyfr codau yn amgryptio geiriau neu ymadroddion cyfan h.y. codau yn amgryptio geiriau neu ymadroddion cyfan, mae seiffrau yn amgryptio llythrennau unigol.

Esbonio: Julius Caesar

Ganed Gaius Julius Caesar yn 100 CC a bu farw yn 44 CC. Cafodd ei lofruddio yn y senedd gan seneddwyr gweriniaethol. Roedd yn wleidydd Rhufeinig, yn unben, yn gadfridog milwrol ac yn hanesydd. Arweiniodd 2 alldaith i Brydain yn 55 CC a 54 CC. Cafodd ei ethol i Gonswl, y safle uchaf yn y fyddin Rufeinig pan oedd yn 40 oed.

Yn ei 20au cafodd ei ddal gan fôr-ladron. Roedd mor garismataidd, tra'n cael ei bridwerthu, ymunodd â'r môr-ladron yn ystod eu gemau a'u hymarferion fel pe bai'n rhan o'r criw. Dywedodd hyd yn oed wrthynt i'w bridwerthu am fwy o arian gan nad oeddent yn gwerthfawrogi ei werth.

Pan dalwyd y pridwerth a'i ryddhau, cododd fflyd o longau a hwylio i'w dal. Ar ôl i'r môr-ladron gael eu carcharu, fe wnaeth Cesar eu tynnu nhw i gyd o'r carchar a'u croeshoelio.

Fel cadfridog milwrol dyfeisiodd ddull amgryptio o'r enw Seiffr Caesar. Mae'n fath o seiffr shifft. Mae pob llythyren yn y testun plaen yn cael ei symud ymlaen gan dri. Yn ystod dadgryptio mae pob llythyren yn cael ei symud yn ôl gan dri.

Tasg: Ffeil Ffeithiau Julius Caesar

Dylai dysgwyr lenwi proffil ffeithiau Julius Caesar yn eu llyfrau gwaith.

Esbonio: Y Seiffr Caesar

Mae Seiffr Caesar yn seiffr shifft gydag allwedd = 3.

Mae hyn yn golygu y bydd hyd yn oed llythyren yn y neges testun plaen yn cael ei symud ymlaen 3 llythyren yn yr wyddor yn ystod amgryptio. Felly mae'r llythyren "A" wedi'i hamgryptio fel y llythyren "D".

I ddadgryptio Seiffr Caesar mae'r derbynnydd yn symud pob llythyren yn y testun seiffr yn ôl 3 llythyren yn yr wyddor. Mae'r llythyren "E" wedi'i dadgryptio i olygu'r llythyren "B".

Enghraifft:

Neges testun plaen: Helo fyd

Testun Seiffr: Khor ibg

Tasg: Torri Allan Olwyn Seiffr

Dylai dysgwyr dorri'r ddwy olwyn allan o'u llyfrau gwaith a'u pinio ynghyd â chaeadwyr papur. Trwy gylchdroi'r olwynion, gall dysgwyr weld y gwahanol wyddor ar gyfer yr allweddi gwahanol.

Tasg: Ymarfer Seiffr Shifft

Dylai dysgwyr geisio dadgryptio'r negeseuon a ddarperir ar y sleidiau ac yn eu llyfrau gwaith.
Datrysiadau:
Allwedd = 3

ehwk bz'u dpvhu pu eodlgg
beth yw'r amser mr blaidd

phqbq klu, phqbq guzj
menyn hir, menyn drwg

Allwedd = 9

lhwcjo r'a onurw pjroo ojud
cyntaf i'r felin gaiff falu

Allwedd = 21

hd rzgvdn evx t yj
mi welais jac y do

Estyniad: Allwedd = 17

Tmy edt od wevod ei qbbuj jy oijohyut, q om'h sqhyqt xmd od qceteb

Dwi ond yn gofyn os allet ti ystyried, a yw'r cariad hwn yn amodol

Trafod: Torri Seiffr Shifft

Trafodwch gyda'r dysgwyr pa mor anodd yw torri seiffr shifft:

- Pa mor anodd ydyn ni'n meddwl yw torri seiffr shifft?
- Faint o allweddi sydd i'w gwirio?
- Pa mor gyflym allwch chi wirio pob allwedd?
- Pa mor gyflym y gallai cyfrifiadur wirio pob allwedd?
- Sut y gallem ei wneud yn fwy anodd?

Esbonio: Seiffrau Trawsosod

Mae'r holl dechnegau cryptograffig yr ydym wedi edrych arnynt hyd yn hyn wedi cynnwys amnewid geiriau neu lythrennau â geiriau/llythrennau/symbolau eraill. Cyfeirir at y rhain fel dulliau amnewid.

Gelwir ail fath o ddull yn ddull trawsosod. Yn lle amnewid y llythyren neu'r geiriau, rydyn ni'n eu cymysgu. Mae hyn yn creu anagram caled iawn y byddai angen ei dorri, oni bai eich bod yn gwybod sut yr ydym wedi aildrefnu'r llythrennau.

Esbonio: Scytale

Yn ôl yn hen Sparta, defnyddiwyd seiffrau trawsosod i anfon negeseuon, gan ddefnyddio silindr pren fel arfer o'r enw scytale.

Crëwyd dau silindr gyda chylchedd union yr un fath, un yn cael ei gadw gan y negesydd ac un yn cael ei gadw gan y derbynnydd.

Roedd darn hir a chul o ddefnydd, lledr fel arfer, wedi'i lapio o amgylch y scytale ac roedd y neges wedi'i hysgrifennu ar ei draws.

Yna caiff y deunydd ei ddadlapio a'i anfon fel un rhestr hir o lythrennau. Mae'r derbynnydd yn lapio'r deunydd o amgylch ei scytale unfath a gall ddarllen y neges.

Estyniad: Scytale

Dylai dysgwyr dorri stribedi hir o bapur. Yna caiff y papur ei lapio o amgylch un o'r scytales a ddarparwyd i amgryptio neges.
Gellir gwneud hyn cwpl o weithiau o flaen y dosbarth fel enghraifft neu mewn parau/tri gydag un dysgwr yn gweithredu fel clustfeiniwr

Dylai fod yn glir pa mor anodd yw hi i ddad-sgrialu hyd yn oed ymadroddion byr, heb sôn am negeseuon cyfan.

Esbonio: Seiffr Rail Fence

Mae Seiffr Rail Fence yn seiffr trawsosod arall. Y tro hwn yn lle dibynnu ar silindrau cylchedd penodol, rydym yn dibynnu ar allwedd a rennir.
Byddwn yn ysgrifennu ein neges mewn patrwm igam ogam ar hyd nifer penodol o reiliau. Yna byddwn yn darllen y neges ar hyd y reiliau a'i hanfon at ein derbynnydd.

I ddadgryptio'r neges, mae'r derbynnydd yn ysgrifennu patrwm igam ogam o flychau yn ôl nifer y rheiliau ac yna'n ysgrifennu'r neges ar draws y rhain, gan ddechrau o'r rheilen uchaf a gweithio i lawr. Ysgrifennu'r neges yn ôl ar draws yr un nifer o reiliau.
Mae nifer y rheiliau yn gweithredu fel yr allwedd yn y system hon.

Er enghraifft:
Allwedd = 4
Testun plaen: MAE HWN YN NEGES CUDD
Testun Seiffr: MYSANNECEWNGUDHED

Tasg: Ymarfer Seiffr Rail Fence

Dylai dysgwyr geisio amgryptio a dadgryptio'r negeseuon a ddarperir ar y sleidiau ac yn eu llyfrau gwaith. Datrysiadau:
Allwedd = 4

MIRMYAANBAGAAYNNSEEEWAHETLATGDTRL
MAE GEN I BEDWAR GATH A MAE'R TY YN LLANAST

HTSOTIDIFEMNOAFYP
HOFFET TI MYND SIOPA

Allwedd = 2

AEHDWHEDCOSEDCHDWH
A OES HEDDWCH HEDDWCH

CNDHBATCNDHBAOEELEIIHEELECLN
CENEDL HEB IAITH CENEDL HEB CALON

Allwedd = 3

MEANAAYIAHNLDYHDUNNWLMEWFAYNI
MAE HEN WLAD FY NHADAU YN ANNWYL I MI

ONNWIGYDRALW
OWAIN GLYNDWR

Estyniad: Allwedd = 5
TFHRNUROAYRUFUMRIBFAORB
TRA MOR YN FUR I'R BUR HOFF BAU

Trafod: Ail-Ymweld

Adolygwch gyda'r dysgwyr y technegau cryptograffig a steganograffig y maent wedi'u dysgu heddiw:
Beth yw'r gwahaniaeth rhwng steganograffeg a cryptograffeg?
Beth yw seiffr Bacon?
Sut ydyn ni'n datgelu inc anweledig?
Beth yw'r gwahaniaeth rhwng cod a seiffr?
Beth yw seiffr pig pen a sut mae'n gweithio?
Beth yw seiffr shifft, sut mae amgryptio a dadgryptio un?
Beth yw Scytale?
Beth yw seiffr Rail Fence, sut mae amgryptio a dadgryptio un?

Tasg: Dianc y Bocs

Mewn grwpiau bach o 5-6, dysgwyr i geisio torri i mewn i'r bocs trwy ddatrys cliwiau a dadgryptio seiffrau sy'n seiliedig ar y technegau a ddysgwyd iddynt hyd yn hyn.
Gosodwch y dasg fel ras rhwng y timau gyda'r tîm cyntaf i orffen yn ennill gwobr.

Pôs 1: Y cod ar gyfer clo rhif un yw'r sifft a ddefnyddir i ddadgryptio'r neges hon wedi'i luosi â'r oedran yr etholwyd Julius Caesar i gonswl
640
Pôs 2: Mae clo rhif 2 yn defnyddio seiffr pig pen. Y cod yw nifer y llythrennau yn yr wyddor, wedi'i luosi â nifer y gridiau a ddefnyddir yn y seiffr pig pen **104**
Pôs 3: NINE NINE SEVEN **997**
Pôs 4: Dyma'r clo olaf, byddwch yn ofalus, mae'n anodd y cod yw naw wyth tri
Ond mae angen troi'r cod o'r pos scytale felly yr ateb = 389

Tasg: Dianc y Bocs

Mae'n bosibl hwyluso'r gweithgaredd hwn trwy brynu cynwysyddion caeadwy a chloeon gyda dolenni hyblyg (fel y gwelir yn y ddelwedd isod.) Gellir gosod y codau ar y cloeon fel y mynnir a gall cael cynwysyddion llai o fewn rhai mwy arwain at bosau a chamau mwy diddorol i'r dysgwyr ei chwblhau.

Mae enghraifft rithwir o'r math hwn o bos i'w weld yn https://scratch.mit.edu/projects/423550886/

Gwahaniaethu ar gyfer Dysgwyr

- Ar gyfer dysgwyr sy'n gweithio tuag at gamau dilyniant gwahanol, gellir addasu dewisiadau seiffrau i weddu.
- Ar gyfer dysgwyr sydd am weithio tuag at gamau dilyniant uwch, darperir estyniadau yn y gweithgareddau sy'n gofyn am fwy o sgiliau datrys problemau megis peidio â darparu'r allwedd. Yn aml rhaid dyfalu yn seiliedig ar geiriau un neu ddau lythyren.
- Mae cyfle hefyd i archwilio seiffrau eraill nas darperir yma megis y seiffr trawsosod colofnol, neu os oes diddordeb gwirioneddol, y seiffr Vignere a seiffr Playfair.

Ble i Fynd Nesaf

- Mae'r adnodd hwn yn canolbwyntio ar ddulliau hanesyddol a chymwysiadau technegau cryptograffig.
- Mae hwn yn gyflwyniad priodol i sut mae cryptograffeg yn cael ei ddefnyddio mewn bywyd bob dydd nawr. Byddai hyn yn cysylltu'n dda â phynciau diogelwch ar-lein a seiberddiogelwch, yn ogystal â thrafodaeth ar y foeseg sy'n ymwneud â sut yr ymdrinnir â'n data personol.
- Gellir archwilio pynciau hacio hefyd, yn enwedig y gwahanol resymau y gallai rhywun geisio cael mynediad at wybodaeth a goblygiadau moesegol a chyfreithiol gwneud hynny.

technocamps

@Technocamps

Find us on Facebook