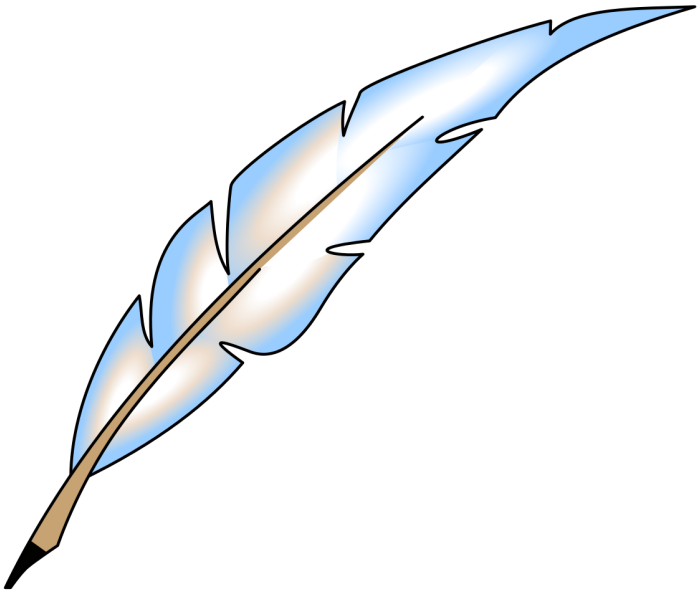
technocamps

Inspiring | Creative | Fun

Ysbrydoledig | Creadigol | Hwyl

Y Dadgodwyr



Swansea University Prifysgol Abertawe

Cardiff University Prifysgol Caerdydd

Prifysgol Bangor University

Cardiff Metropolitan University | Prifysgol Metropolitan Caerdydd

i.t.wales www.itwales.com

Prifysgol Aberystwyth University

Prifysgol Glyndŵr University

University of South Wales Prifysgol De Cymru

Yn gweithio ar ran Llywodraeth Cymru

Working on behalf of the Welsh Government

Amcanion

- I ddysgu sut i ddefnyddio amgryptio i ysgrifennu negeseuon cudd.
- I ddysgu sut defnyddiwyd cod yn ystod y Rhyfel Byd Cyntaf.
- I ddysgu sut i ddadgryptio negeseuon cudd gan ddefnyddio tair dull wahanol.

Trosolwg

Yn y gweithdy hwn, byddwn yn edrych ar ddull penodol o ysgrifennu negeseuon cudd na fydd neb arall yn eu deall! Defnyddiwyd y dull hwn ers cannoedd o flynyddoedd a byddwn yn edrych ar sut y defnyddiwyd codau cyfrinachol yn ystod y Rhyfel Byd Cyntaf.

Byddwn yn dysgu sut i ysgrifennu negeseuon cudd, sut i gyfrifo'r hyn y mae neges gyfrinachol yn ei olygu wrth ddefnyddio tri dull, ac yn olaf byddwn ni'n defnyddio'r sgiliau hyn i helpu'r ymdrechion rhyfel!

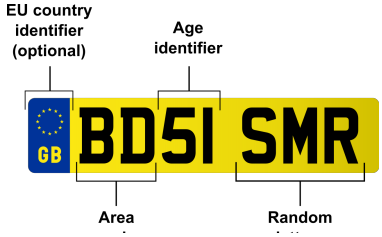
Geiriau Allweddol

Amgryptio
Allwedd
Olwyn Seiffr
Dadgryptio
Cod

Amgryptio – Defnyddio symbolau, llythyrau neu rifau, neu ail-drefnu llythrennau i guddio neges.
Dadgryptio – Defnyddio dull i weithio allan beth mae neges guddiedig yn ei olygu, rhan fwyaf o'r amser gan ddefnyddio allwedd.
Allwedd – Allwedd yw darn o wybodaeth a ddefnyddir i amgryptio neu ddadgryptio neges. Fel cloi a datgloi drws, bydd defnyddio allwedd wahanol i ddatgloi drws ddim yn gweithio, rhaid iddo fod yr un peth. Hyd yn oed os ydym yn gwybod sut i agor y clo, ni allwn ni barhau heb yr allwedd gywir.
Cod – Mae cod yn amnewid geiriau, ymadroddion neu frawddegau gyda grwpiau o lythrennau neu rifau.
Olwyn Seiffr – Olwyn gyda llythrennau neu symbolau y gellir eu defnyddio i amgryptio neges yn hawdd. Rhoddir yr allwedd gan faint y mae'r olwyn yn cael ei droi.

Cod Pob Dydd

Yn ein bywydau bob dydd, rydym yn gweld codau ym mhob man, ond efallai na fyddwn yn sylweddoli hynny! Defnyddir cod er mwyn cyfathrebu gwybodaeth mewn ffordd fyrrach neu haws. Mae platiau cofrestru ceir yn un enghraifft, codau post, codau bar ar eitemau mewn siopau, Codau QR, mae'r rhain i gyd yn enghreifftiau o'r cod a welwn o'n cwmpas.

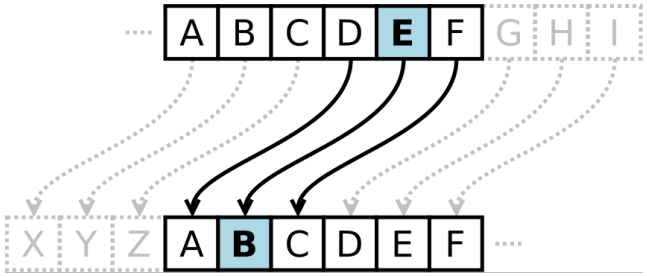


Ysgrifennwch restr yn y blwch hwn neu llenwch y diagram corryn isod:

Y Seiffr Caesar

Mae'r seiffr Caesar, a elwir hefyd yn seiffr shifft, yn un o'r ffurfiau hynaf a symlaf o amgryptio neges.

Mae'n fath o seiffr amnewid lle mae pob llythyren yn y neges wreiddiol (sy'n cael ei alw'n testun plaen, *plaintext*) yn cael ei amnewid gyda llythyren sy'n cyfateb i nifer penodol o lythrennau i fyny neu i lawr yn yr wyddor.



Defnyddiodd Julius Caesar (y mae'r cipher wedi'i enwi ar ei gyfer) hyn trwy symud y llythrennau yn yr wyddor gan 3 lle, felly mae D yn dod yn A, ac E yn dod yn B ac yn y blaen. Golygai hyn na allai neb ddarllen negeseuon yn gyflym nad oeddent i fod os mai dim ond cipolwg cyflym oedd ganddynt.

Amgryptio Gyda'r Seiffr Caesar

Ar hyn o bryd, dylech gael Olwyn Seiffr i'ch helpu i amgryptio eich neges. Os na, gallwch ddod o hyd i gopi digidol yn y Gêm Scratch yn http://bit.ly/CipherWheel neu fersiwn argraffadwy yn https://bit.ly/technocampsTWF

1. Amgryptiwch "Y Bluen Wen" gan ddefnyddio Shifft Caesar o 3.

Y B L U E N W E N

2. Amgryptiwch cyfenw eich athro neu athrawes gyda shifft o 3.

3. Amgryptiwch enw rhywun o'ch ysgol gan ddefnyddio shifft o naill ai 3 neu 4.

Dadgryptio gyda'r Seiffr Caesar

Nawr eich bod chi'n arbenigwr mewn amgryptio, ceisiwch ddefnyddio dadgryptio i ddarllen y negeseuon cudd isod:

1. L W U L H G. L U H D O O B W U L H G.

2. L G R Q R W Z D Q W B R X U Z D U.

3. L ' P V X U U R X Q G H G E B J K R V W V.

4. (Hint: Efallai nid shifft o 3 yw hwn!)
Q M P I W X S K S F I J S V I M W P I I T

Beth Ydy Hwn Yn Ymwneud A'r Rhyfel?

A allwch chi feddwl am unrhyw gysylltiad rhwng yr hyn yr ydym wedi'i edrych ar hyd yn hyn a'r Rhyfel Byd Cyntaf?

Sut y gallai codlyfr helpu i ddadgryptio negeseuon cyfrinachol?

A oes unrhyw anfanteision i ddefnyddio llyfr cod?

Darlledwyd enghraifft arall o godau a ddefnyddiwyd, tro hwn yn ystod yr Ail Ryfel Byd, ar sioeau radio iaith Ffrangeg o Lundain. I'r rhan fwyaf o bobl, mae'n ymddangos fel negeseuon ddiystyr (a braidd yn wirion). Beth ydych chi'n meddwl y gallent ei olygu?

Bydd Clementine yn darganfod basged o wyau wrth ei drws.

Mae gan Jean mwstas mawr.

Dulliau Dadgryptio

O ran seiffrau, mae seiffr Caesar (math o seiffr amnewid) yn un o'r symlaf, sy'n golygu na chaiff ei ddefnyddio yn aml. Gall cyfrifiadur dorri neges ac amgryptiwyd gyda seiffr Caesar yn gyflym iawn. Mae yna sawl ffordd o wneud hyn a byddwn yn archwilio ychydig ohonynt isod.

Y dull gyntaf, yw torri cod trwy wybod yr allwedd. Edrychwch ar y nodyn isod a gweld a allwch chi weithio allan sut i'w ddadgryptio.

(7)

APT

P OHCL H ZLJYLA
SLA'Z TLLA
KHU

Nawr beth am os nad oes gennym yr allwedd? A oes unrhyw beth arall a all ein helpu ni? Rhowch gynnig ar y nodyn isod. (Pa lythyren a allai fod yn 'M' ar ei ben ei hun? A allwn ni gael allwedd o hyn?)

M PMOI WEVEL,
FYX HSR'X XIPP
LIV M WEMH WS.

Tasg Estynedig: Dadansoddiad Amlder

Dadansoddiad amlder yw'r term ar gyfer edrych ar y llythrennau neu'r symbolau i weld pa un sy'n ymddangos fwyaf. Yn yr iaith Saesneg, y llythyren sy'n ymddangos yn fwyaf aml yw'r llythyren "E". Golyga hyn, trwy gyfri'r llythrennau a gweld pa rai sy'n ymddangos fwyaf, ac yna gosod yr allwedd er mwyn iddo gyfateb â'r llythyren "E", gallwn ddod o hyd i'r allwedd gywir.

EWWLEWGMLKAVWLZ

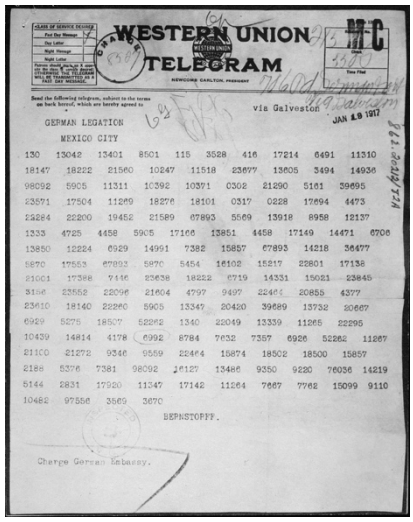
WYSLWLZAKWNWFAFY

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

Beth ydy'r neges yn dweud? Allwedd : _____

Room 40 A'r Telegram Zimmerman

Yn ystod y Rhyfel Byd Cyntaf, roedd codau, seiffrau a cryptograffeg wedi dod yn hanfodol wrth sicrhau bod cyfathrebiadau yn cael eu cadw'n gyfrinachol. Oherwydd hyn, chwaraeodd dadgryptio rôl hanfodol yn ymdrechion rhyfel ar y ddwy ochr. Sefydlodd y Prydeinig grŵp o bobl â'u rôl oedd dadgryptio codau Almaeneg. Roedd hwn yn waith pwysig a arweiniodd at wybodaeth bwysig o'r Almaen yn cael ei ddwyn a'i ddefnyddio i'w fantais. Gelwir y grŵp hwn yn "Room 40" ac arweiniodd un dogfen benodol at UDA yn ymuno â'r ymdrech Rhyfel.


WESTERN UNION
TELEGRAM

vis Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 07893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 9446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2186 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

Y Telegram Zimmerman

Roedd y Telegram Zimmerman yn neges wedi'i hamgryptio a anfonwyd ym 1917, gan yr Almaen i Fecsico, gan geisio eu perswadio i'w ymuno trwy fynd i ryfel gyda'r UDA os oeddent yn ymuno â Phrydain. Fodd bynnag, cafodd y neges ei ddwyn gan Brydain cyn iddo groesi'r Iwerydd i'r UDA ac ymlaen i Fecsico. Fe'i dadgodiwyd wedyn gan ddynion a menywod Room 40. Yna, roedd yn rhaid i Brydain esgus bod un o'u ysbïwyr wedi dwyn y telegram gan nad oeddent am i'r UDA wybod eu bod yn dwyn eu cyfathrebiadau! Nid oedd yr UDA yn rhy hapus am y Telegram ac ymunodd â'r Rhyfel ym 1917, er na roddodd Prydain wybod iddynt eu bod yn edrych ar eu negeseuon am flynyddoedd lawer!

Stopio'r bom!

Defnyddiwch y gwagle fan hyn i dadgryptio'r negeseuon a rhoddir i chi!

Neges A:

Neges B:

Neges C:

Neges D:

Neges E: