technocamps

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

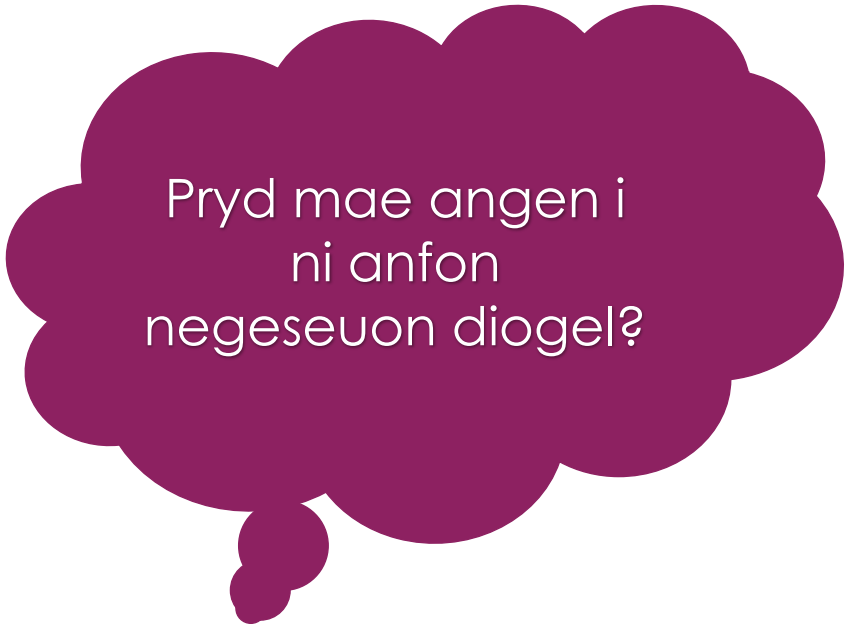
PRIFYSGOL glyndŵr Wrecsam
Wrexham glyndŵr UNIVERSITY

University of South Wales
Prifysgol De Cymru

technocamps

Cryptograffeg

Tasg: Cynllun Corryn



Beth yw Steganograffeg?

Steganograffeg

Steganograffeg yw'r arfer o guddio negeseuon neu wybodaeth o fewn negeseuon neu wybodaeth gyfrinachol eraill. Daw **Steganograffeg** o'r "Steganos" Groegaidd, sy'n golygu cuddio neu orchuddio, a "Graphein", sy'n golygu ysgrifennu.

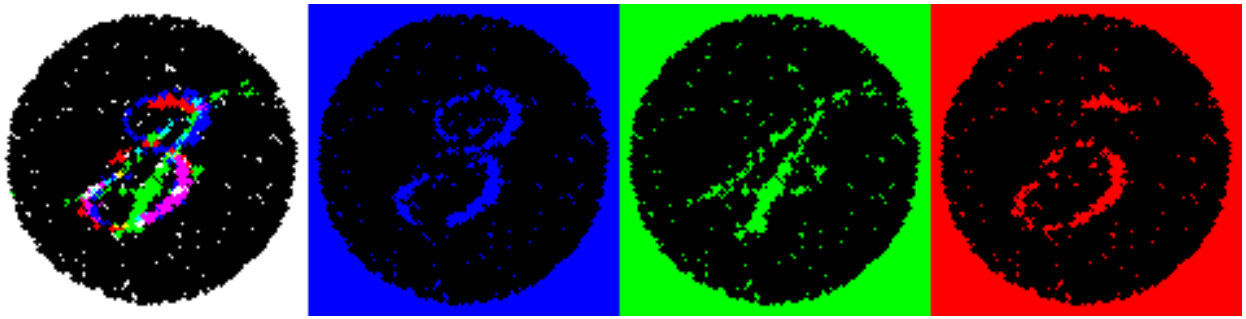
Defnyddir **steganograffeg** i ddyfrnodi fideos a lluniau yn ddigidol ac weithiau fe'u defnyddir i **anfon negeseuon cudd.**

Dyma rai enghreifftiau pan ddefnyddir **Steganograffeg:**

T***hi***s is ***an*** e***xa***mple ***o***f h***o***w to ***hid***e a ***m***e***s******ag***e ***wi***th***in a*** messag***e*** u***si******n***g th***e*** Ba***co***n c***o***de

Steganograffeg

Mae Steganograffeg yn gweithio oherwydd nad yw'r clustfeini (eavesdropper) yn gwybod ble mae'r neges wedi'i chuddio ac efallai nad yw'n gwybod bod neges gudd hyd yn oed yna yn y lle cyntaf!



Tasg: Diffinio Steganograffeg

Gwas Histiaeus

Yn ôl yng Ngwlad Groeg hynafol (ancient Greece), roedd Histiaeus eisiau anfon neges at ei ffrind.

Ond roedd yn poeni y byddai'r neges yn cael ei rhyng-gipio a'i darllen gan ei elynion.

Pe bai'r neges wedi'i hysgrifennu ar ddarn plaen o bapur, byddai'n cael ei darganfod a'i darllen yn gyflym pe bai'r negesydd yn cael ei ddal a'i chwilio.

Gwas Histiaeus

Felly roedd angen i Histiaeus guddio'r neges.

Fe eilliodd (shaved) ben ei was yr ymddiriedir ynddo fwyaf a thatŵio'r neges ar gefn eu pen.

Pan fyddai gwallt y gwas wedi tyfu'n ôl, byddai'r neges yn cael ei chuddio.

Pe bai'r negesydd yn cael ei ddal a'i chwilio, ni fyddai modd dod o hyd iddo.

Tasg: Gwas Histiaeus

Problemau Gyda'r System?

Syr Francis Bacon

Cododd y syniad y dylai gwybodaeth fod yn seiliedig ar resymu ac arsylwadau anwythol yn unig, a elwir hefyd yn **Y Dull Gwyddonol.**

Lluniodd ddull Steganograffig o guddio negeseuon trwy ddefnyddio gwahanol ffontiau.

Y Seiffr Bacon

Mae'r **Seiffr Bacon** yn ddull o guddio neges y tu mewn i neges arall trwy newid ffontiau.

1. Ysgrifennwch y neges rydyn ni am ei chuddio.
2. Dewiswch 2 fath gwahanol o ffont, A a B, fel **print trwm** ac *italig* neu ***Comic Sans*** ac *Edwardian Script*.
3. Ysgrifennwch neges ddiflas gydag o leiaf 5 gwaith cymaint o lythrennau ynddo â'r neges gudd.
4. Newidiwch ffont y neges ddiflas o arddull A i B ar gyfer pob un o'r llythrennau cyfatebol yn y neges gudd.

Enghraifft

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	

Neges Bacon: ES i i'r YsgoL HEdDiW, RoEdD hI'N BWRW GIAW AC YN WLyB lawn YCh a Fi!

Enghraifft

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	

Neges Bacon: ES i i'r YsgoL HEdDiW, RoEdD hI'N BWRW GIAW AC YN WLyB lawn YCh a Fi!

Math Ffont A: PRIFLYTHRENNAU

Math Ffont B: llythrennau bach

Enghraifft

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	

Neges Bacon: ES i i'r YsgoL HEdDiW, RoEdD hI'N BWRW GIAW AC YN WLyB lawn YCh a Fi!

Math Ffont A: PRIFLYTHRENNAU

Math Ffont B: llythrennau bach

Wedi Cyfieithu: AABBB

Neges Cudd: H

Enghraifft

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	

Neges Bacon: ES i i'r YsgoL HEdDiW, RoEdD hI'N BWRW GIAW AC YN WLyB lawn YCh a Fi!

Math Ffont A: PRIFLYTHRENNAU

Math Ffont B: llythrennau bach

Wedi Cyfieithu: AABBB ABBBA

Neges Cudd: HO

Enghraifft

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	

Neges Bacon: ES i i'r YsgoL HEdDiW, RoEdD hI'N BWRW GIAW AC YN WLyB lawn YCh a Fi!

Math Ffont A: PRIFLYTHRENNAU

Math Ffont B: llythrennau bach

Wedi Cyfieithu: AABBB ABBBA AABAB

Neges Cudd: HOF

Enghraifft

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	

Neges Bacon: ES i i'r YsgoL HEdDiW, RoEdD hI'N BWRW GIAW AC YN WLyB lawn YCh a Fi!

Math Ffont A: PRIFLYTHRENNAU

Math Ffont B: llythrennau bach

Wedi Cyfieithu: AABBB ABBBA AABAB AABAB

Neges Cudd: HOFF

Enghraifft

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	

Neges Bacon: ES i i'r YsgoL HEdDiW, RoEdD hI'N BWRW GIAW AC YN WLyB lawn YCh a Fi!

Math Ffont A: PRIFLYTHRENNAU

Math Ffont B: llythrennau bach

Wedi Cyfieithu: AABBB ABBBA AABAB AABAB

Neges Cudd: HOFFi BACON

Tasg: Ymarfer Seiffr Bacon

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	

1. Yr aMSEr yw CHWEcH O'R gloch YN SlapAn

2. YDY, mAE LLAEtH Yn fLAsus

3. RHEDeg Yn hWyR EtO

4. yDych Chi'n DIGOn DDEwr i Roi GyNnig AR YR uN HON, NEU ydY Hl'n eich OFnl?

Problemau gyda'r Seiffr Bacon?

Tasg Estyniad: Gwneud Eich inc Anweledig Eich Hun

Ail-Ymweld

Tasg: Beth Yw Cryptograffeg?

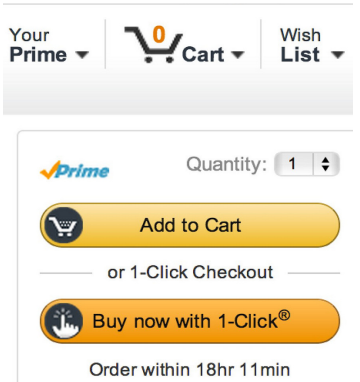
Cryptograffeg

Cryptograffeg yw ymarfer ac astudio technegau ar gyfer cyfathrebu diogel.

Daw **cryptograffeg** o'r "Kryptos" Groegaidd, sy'n golygu cyfrinach neu gudd, a "Graphein", sy'n golygu ysgrifennu.

Defnyddir **technegau cryptograffig** trwy'r amser ym mywyd pob dydd heb i chi hyd yn oed sylwi.

Dyma rai enghreifftiau o pryd y defnyddir **Cryptograffeg**:

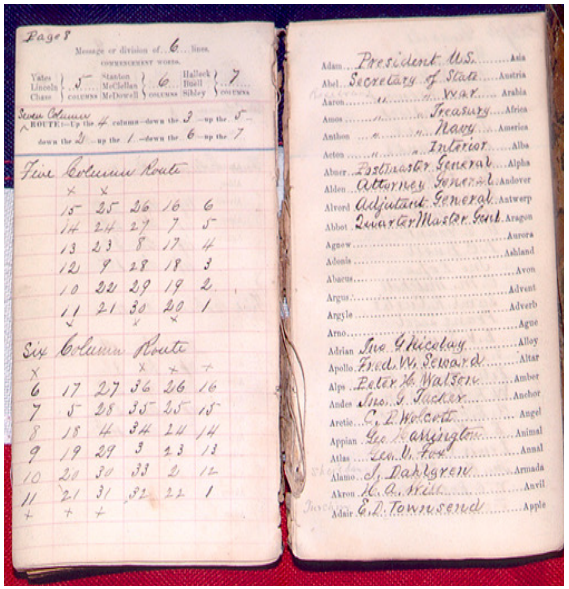


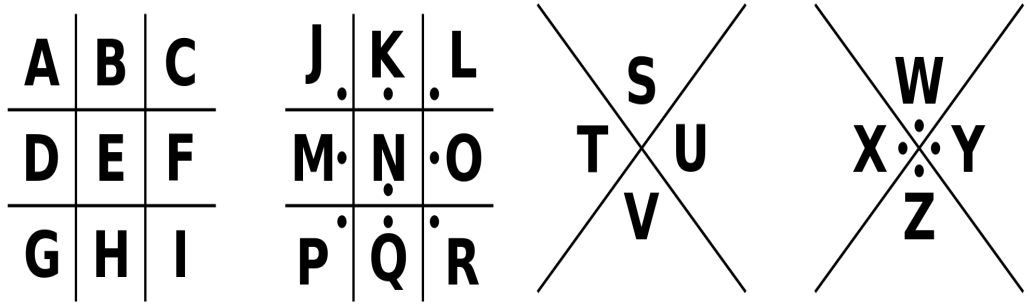
Cryptograffeg

Mae **cryptograffeg** yn wahanol i **steganograffeg**.

Mewn **cryptograffeg**, gall pawb ddweud bod neges gyfrinachol wedi'i hanfon.

Daw'r diogelwch o'r anhawster wrth **ddadgryptio'r** neges heb wybod yr **allwedd** benodol a ddefnyddiwyd.





Tasg: Diffinio Cryptograffeg

Codlyfrau

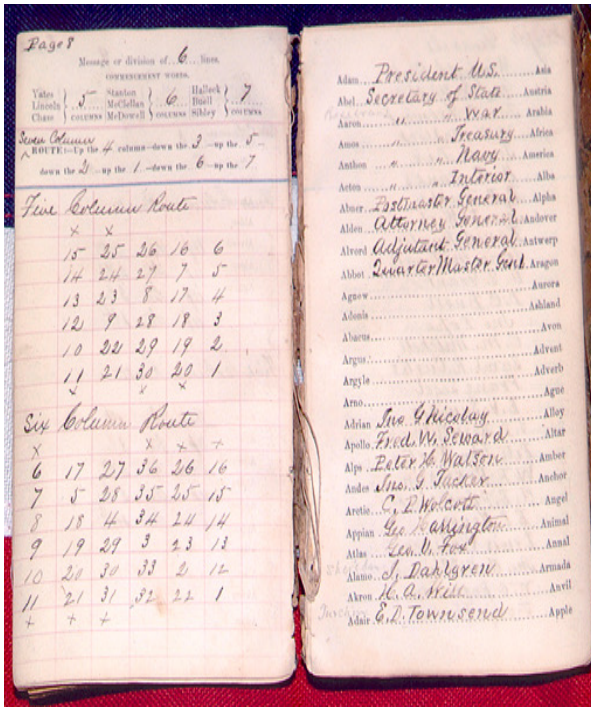
Mae un dull cryptograffig a ddefnyddir yn gyffredin yn seiliedig ar **lyfrau cod**.

Rydyn ni'n ysgrifennu llyfr cyfan math geiriadur sy'n newid ystyr geiriau neu ymadroddion.

Mae gennym gopi ac mae gan y derbynnydd gopi.

Rydym yn ysgrifennu ein neges ac yn **amgryptio** pob gair neu ymadrodd yn y neges yn ôl ein **codlyfr**.

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



technocamps

Tasg: Gwnewch Eich Codlyfr Eich Hun

Siaradwyr Cod

Mae **codlyfrau** fel cyfieithu i iaith arall, gan dybio nad yw rhywun sy'n rhyng-gipio'r neges yn siarad yr iaith wedi'i **hamgryptio**.

Defnyddiwyd y syniad hwn yn ystod y ddau ryfel byd fel techneg amgryptio.

Yn rhyfeddol, defnyddiwyd Cymraeg hyd yn oed at y dibenion hyn gan nad oes llawer o bobl y tu allan i Gymru yn gallu siarad Cymraeg.

Navajo

Y defnydd mwyaf cyffredin o gyfieithu i iaith arall oedd gyda phobl Navajo.

Yn yr Ail Ryfel Byd, rhoddwyd aelodau o boblogaeth Navajo mewn gwahanol blatwnau i anfon negeseuon wedi'u **hamgryptio** trwy gyfieithu'r neges Saesneg i Navajo.

Gan mai ychydig iawn o bobl y tu allan i gymuned fach y Navajo sy'n gallu siarad Navajo, roedd y Siapaneaid o'r farn bod y cod yn amhosibl ei dorri.

NAVAJO CODES
NAME OF SHIPS

SHIPS	TOH-DINEH-IH	SEA FORCE
BATTLESHIP	LO-TSO	WHALE
AIRCRAFT	TSIDI-MOFFA-YE-HI	BIRD CARRIER
SUBMARINE	BESH-LO	IRON FISH
MINE SWEEPER	CHA	BEAVER
DESTROYER	CA-LO	SHARK
TRANSPORT	DINEH-NAY-YE-HI	MAN CARRIER
CRUISER	LO-TSO-YAZZIE	SMALL WHALE
MOSQUITO BOAT	TSE-E	MOSQUITO

NAVAJO CODES
NAME OF PLANES

PLANES	WO-TAH-DE-NE-IH	AIR FORCE
DIVE BOMBER	GINI	CHICKEN HAWK
TORPEDO PLANE	TAS-CHIZZIE	SWALLOW
OBS. PLAN	NE-AS-JAH	OWL
FIGHTER PLANE	DA-HE-TIH-HI	HUMMING BIRD
BOMBER PLANE	JAY-SHO	BUZZARD
PATROL PLANE	GA-GIH	CROW
TRANSPORT	ATSAH	EAGLE

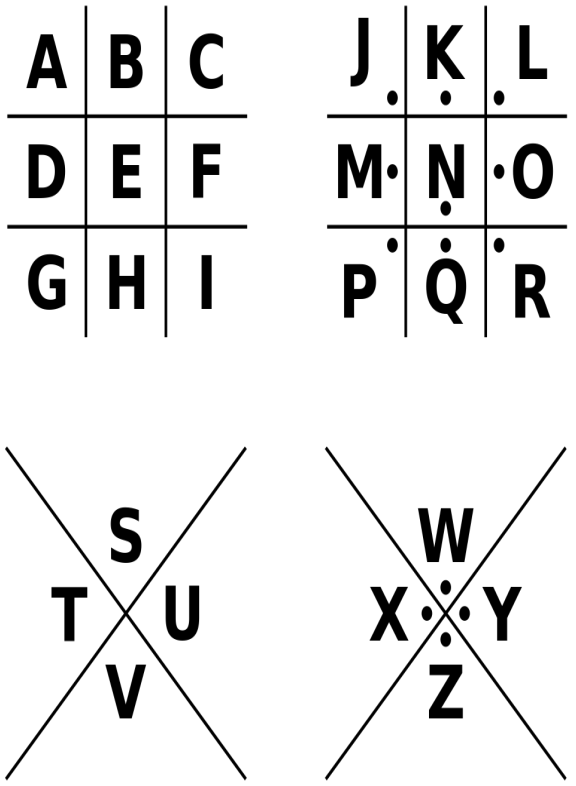
Seiffr Pig Pen

Mae seiffr **Pig Pen** wedi cael ei ddefnyddio trwy gydol hanes gan grŵp cudd o'r enw'r Seiri Rhyddion (Freemasons)

Mae'r Seiri Rhyddion yn debyg i glwb cudd. Mae ganddyn nhw ysgwyd llaw, codau a defodau (rituals) cyfrinachol nad ydyn nhw i fod i'w rhannu gyda'r byd y tu allan.

Mae pob llythyren yn eich neges **plaintext** wedi'i **hamgryptio** gan ddefnyddio'r grid.

Anfonir y symbolau rhyfedd wrth i'r neges a'r derbynnydd eu **dadgryptio**.



Tasg: Ymarfer Pig Pen

Codau vs. Seiffrau

Codau vs. Seiffrau

Mae codau yn **amgryptio** geiriau a / neu ymadroddion cyfan yn y **plaintext** ac yn **dadgryptio** geiriau a / neu ymadroddion cyfan yn y **ciphertext**.

Mae seiffrau yn **amgryptio** llythrennau unigol yn y **plaintext** ac yn **dadgryptio** llythrennau unigol yn y **ciphertext**.

Côd:

Mae Prydain yn ymuno â'r rhyfel -> Mae gan Jean barf enfawr

Seiffr:

Helo fy enw i yw Luke -> 

Julius Caesar

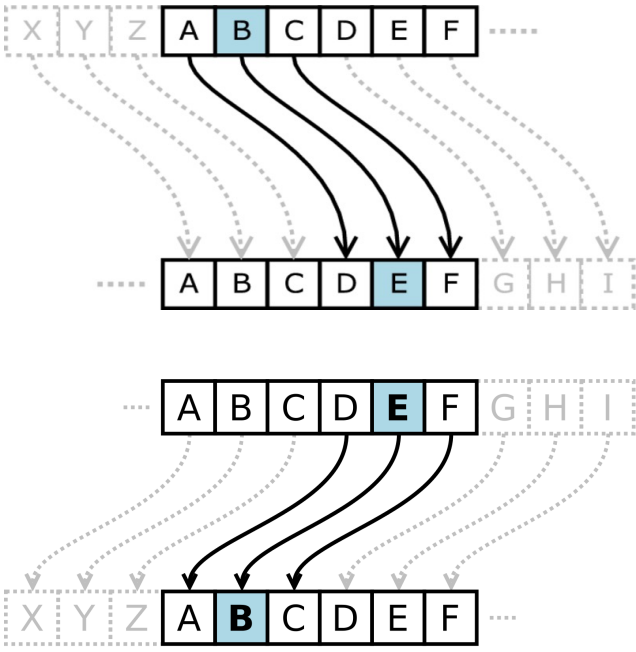
Gaius Julius Caesar:

- 100 CC – 44 CC
- Gwleidydd Rhufeinig, unben, cadfridog milwrol a hanesydd.
- Arweiniodd 2 alldaith i Brydain yn 55 CC a 54 CC.
- Etholwyd i Gonswl, y safle uchaf ym myddin y Rhufeiniaid, pan oedd yn 40 oed.
- Yn ei 20au cafodd ei gipio gan fôr-ladron.
- Llofruddiwyd yn y Senedd gan seneddwyr gweriniaethol.
- Fel cadfridog milwrol dyfeisiodd ddull o amgryptio a elwir y seiffr Caesar.

Tasg: Ffeil
Ffeithiau
Julius Caesar

Seiffr Caesar

Mae'r **seiffr Caesar** yn **seiffr shifft** gydag **allwedd 3**.



Yn ystod amgryptio, mae pob llythyren yn y neges **plaintext** yn cael ei symud ymlaen 3 llythyren yn yr wyddor. **Amgryptir** y llythyren "A" fel y llythyren "D".

Yn ystod dadgryptio, mae'r derbynnydd yn symud pob llythyren mewn **ciphertext** yn ôl 3 llythyren. Mae'r llythyren "E" wedi'i **ddadgryptio** i olygu'r llythyren "B".

Er enghraifft:

Plaintext:	Hello world
Ciphertext:	Khoor zruog

Tasg: Torri Allan Olwyn Seiffr

Tasg: Ymarfer Seiffr Shifft

Seiffr Caesar, Allwedd = 3:

- **ehwk bz'u dpvhu pu eodlgg**
- **phqbq klu, phqbq guzj**

Allwedd = 9:

- **lhwcjo r'a onurw pjroo ojud**

Allwedd = 21:

- **hd rzgvdn evx t yj**

Estyniad: Ni roddir allwedd

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

technocamps

Pa Mor Anodd Yw Torri Seiffr Shifft?

Seiffrau Trawsosod

Hyd yn hyn mae'r holl **dechnegau cryptograffig** wedi cynnwys amnewid geiriau neu lythrennau â geiriau neu lythrennau eraill. Gellir meddwl am y rhain fel **dulliau amnewid.**

Beth petaem yn cymysgu trefn y llythyrau yn lle?

Byddem yn creu anagram caled iawn y mae angen ei dorri, oni bai eich bod yn gwybod sut y gwnaethom eu cymysgu.

Gelwir y rhain yn **seiffrau trawsosod**.

M						Y						S				
	A				N		N				E		C			
		E		W				N		G				U		D
			H						E						D	

Scytale

Yn ôl yn Sparta hynafol, defnyddiwyd **seiffrau trawsosod** i anfon negeseuon gan ddefnyddio silindr pren o'r enw **Scytale**.

1. Crëwyd dau silindr union yr un fath.

2. Roedd darn hir a chul o ddeunydd, lledr fel arfer, wedi'i lapio o amgylch y **Scytale** ac ysgrifennwyd y neges ar ei draws.

3. Ar ôl i'r neges gael ei hysgrifennu, roedd y deunydd yn cael ei ddad-rolio a'i anfon fel un rhestr hir o lythyrau.

4. Fe lapiodd y derbynnydd y neges o amgylch ei **Scytale** unfath a darllen y neges.

Tasg Estyn: Scytale

Seiffr Rail Fence

Mae'r **seiffr Rail Fence** yn **seiffr trawsosod** arall.

1. Ysgrifennwch y neges mewn patrwm tebyg i igam-ogam ar nifer penodol o "reiliau".
2. Darllenwch y neges ar hyd y reiliau a'i hanfon at y derbynnydd.
3. Mae'r derbynnydd yn ysgrifennu'r neges yn ôl ar draws yr un nifer o reiliau ac yn darllen y neges.

Mae nifer y rheiliau yn gweithredu fel yr **allwedd** yn y system hon.

Er enghraifft:

Allwedd = 4

Plaintext: MAE HWN YN NEGES CUDD

Ciphertext: MYSANNECEWNGUDHED

M						Y						S				
	A				N		N				E		C			
		E		W				N		G				U		D
			H						E						D	

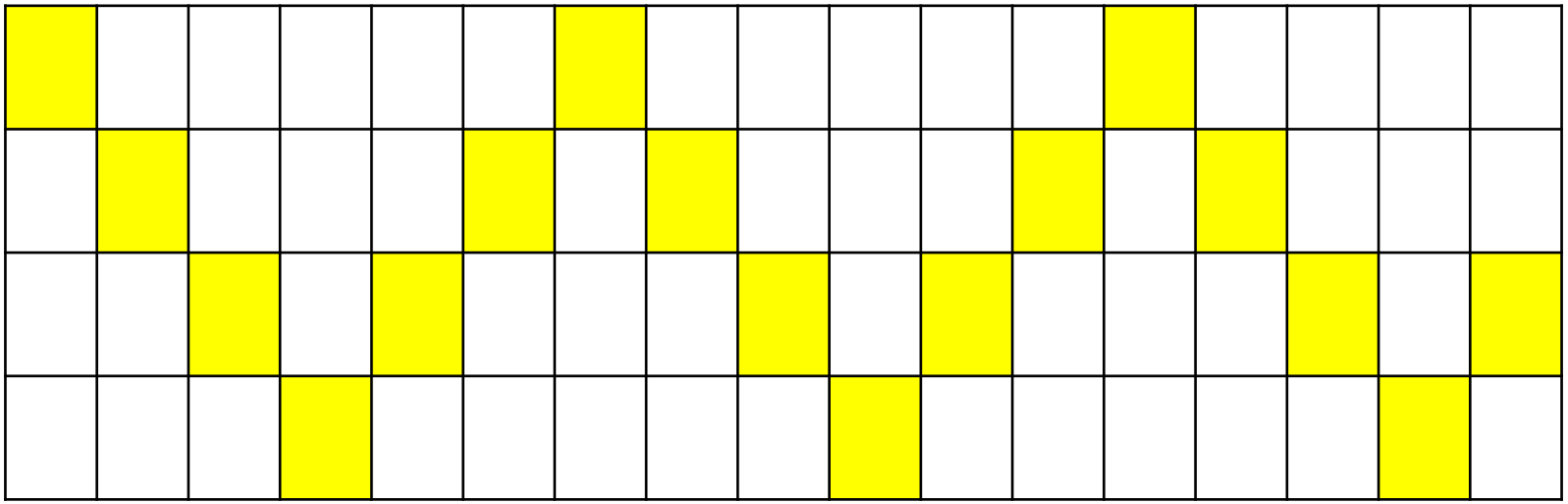
Enghraifft o Seiffr Rail Fence

Dywedwch mai'r neges oedd “MYSANNECEWNGUDHED” a'r allwedd oedd pedair.

Enghraifft o Seiffr Rail Fence

Dywedwch mai'r neges oedd “MYSANNECEWNGUDHED” a'r allwedd oedd pedair.

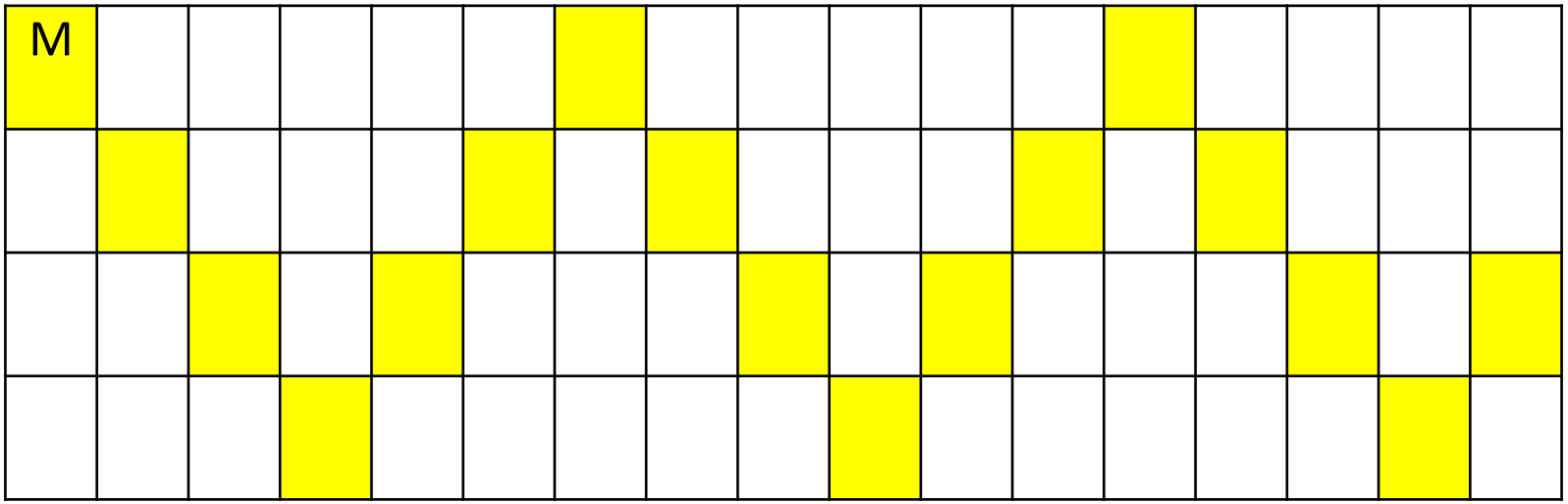
Lluniwch igam ogam ar hyd y 4 rheilen gyda chymaint o flychau â llythrennau yn y neges.



Enghraifft o Seiffr Rail Fence

Rydyn ni'n ysgrifennu'r neges ar hyd pedair rheilen yn y blychau cywir a roddwyd i ni gan batrwm igam-ogam.

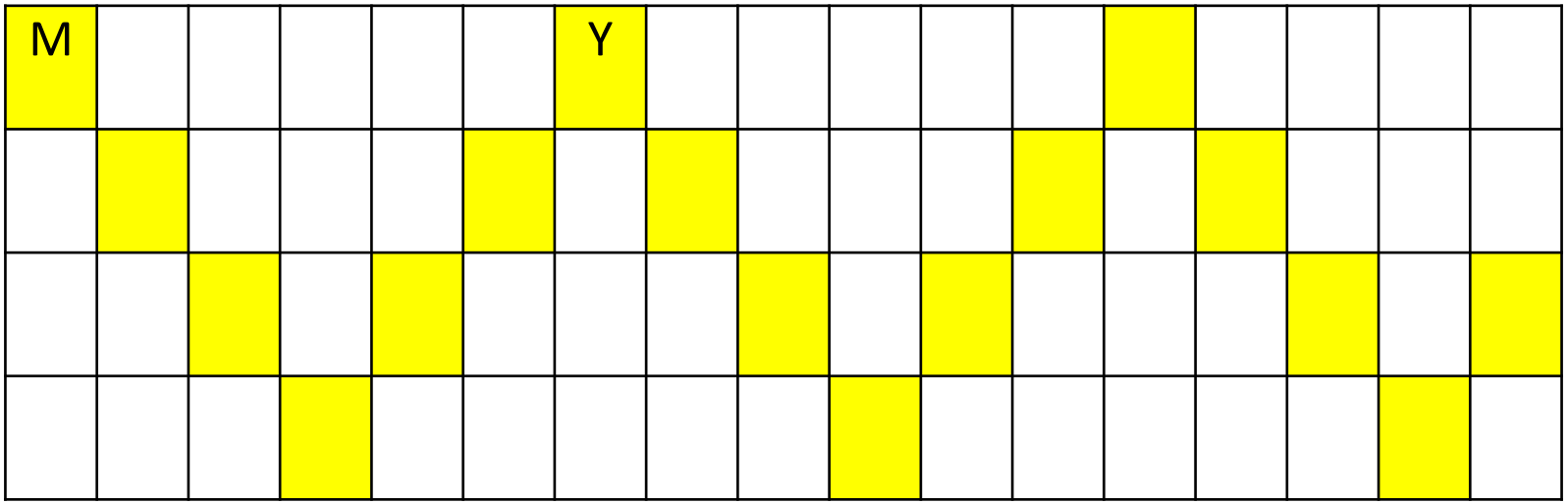
Neges: “MYSANNECEWNGUDHED”



Enghraifft o Seiffr Rail Fence

Rydyn ni'n ysgrifennu'r neges ar hyd pedair rheilen yn y blychau cywir a roddwyd i ni gan batrwm igam-ogam.

Neges: “MYSANNECEWNGUDHED”



Enghraifft o Seiffr Rail Fence

Rydyn ni'n ysgrifennu'r neges ar hyd pedair rheilen yn y blychau cywir a roddwyd i ni gan batrwm igam-ogam.

Neges: “MYSANNECEWNGUDHED”

M						Y						S			

Enghraifft o Seiffr Rail Fence

Rydyn ni'n ysgrifennu'r neges ar hyd pedair rheilen yn y blychau cywir a roddwyd i ni gan batrwm igam-ogam.

Neges: “MYSANNECEWNGUDHED”

M						Y						S				
	A															

Enghraifft o Seiffr Rail Fence

We write out the message along four rails in the correct boxes given to us by a zig zag pattern.

Message: "MYSANNECEWNGUDHED"

M						Y						S				
	A				N		N				E		C			

Enghraifft o Seiffr Rail Fence

Rydyn ni'n ysgrifennu'r neges ar hyd pedair rheilen yn y blychau cywir a roddwyd i ni gan batrwm igam-ogam.

Neges: “MYSANNECEWNGUDHED”

M						Y						S				
	A				N		N				E		C			
		E		W				N		G				U		D

Enghraifft o Seiffr Rail Fence

Rydyn ni'n ysgrifennu'r neges ar hyd pedair rheilen yn y blychau cywir a roddwyd i ni gan batrwm igam-ogam.

Neges: “MYSANNECEWNGUDHED”

M						Y						S				
	A				N		N				E		C			
		E		W				N		G				U		D
			H						E						D	

Enghraifft o Seiffr Rail Fence

Yna darllenir y neges wedi'i dadgryptio ar hyd y igam-ogam a chawn "MAE HWN YN NEGES CUDD"

M						Y						S				
	A				N		N				E		C			
		E		W				N		G				U		D
			H						E						D	

Tasg: Ymarfer Seiffr Rail Fence

Dadgryptio'r Negeseuon Hyn

Allwedd = 4:

- **MIRMYAANBAGAAYNNSEEEWAHETLATGDTRL**
- **HTSOTIDIFEMNOAFYP**

Allwedd = 2:

- **AEHDWHEDCOSEDCHDWH**
- **CNDHBATCNDHBAOEELEIIHEELECLN**

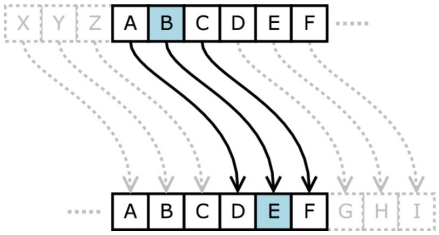
Allwedd = 3:

- **MEANAAYIAHNLDYHDUNNWLMEWFAYNI**
- **ONNWIGYDRALW**

Estyniad: Ni roddir allwedd

- **TFHRNUROAYRUFUMRIBFAORB**

Ail-Ymweld

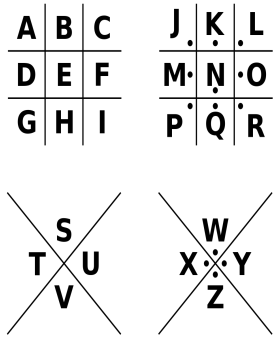


Mae Steganograffeg yn cuddio negeseuon y tu mewn i negeseuon eraill. Ymhlith yr enghreifftiau mae: inc anweledig, gwas Histiaeus a seiffr Bacon.

Mae cryptograffeg yn anfon negeseuon yn ddiogel. Wedi'i rannu'n ddau brif grŵp: Amnewid a Thrawsosod.

Mae enghreifftiau o ddulliau Amnewid yn cynnwys: Seiffr Caesar, Seiffr pig pen a codlyfrau.

Mae enghreifftiau o ddulliau trawsosod yn cynnwys: Seiffr Rail Fence a Scytale.



Tasg: Dianc o'r Blwch