Twyll-len Cryptograffeg

Seiffr Bacon

Dewiswch eich neges gudd.
Dewiswch ddwy ffont a'u labelu A a B.
Ysgrifennwch neges ddiflas gyda 5 gwaith cymaint o lythrennau â'r neges gudd.
Amgodiwch eich neges gudd gan ddilyn y tabl isod trwy newid ffontiau eich neges ddiflas o A i B yn dilyn sut mae'r neges gudd wedi'i amgodio.

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 gudd: Hoffi Bacon
Neges arferol: Es i i'r ysgol heddiw, roedd hi'n bwrw glaw ac yn wlyb iawn, ych a fi!
Math Ffont A: PRIFLYTHRENNAU
Math Ffont B: llythrennau bach

Neges gudd wedi'i hamgáu (enciphered):

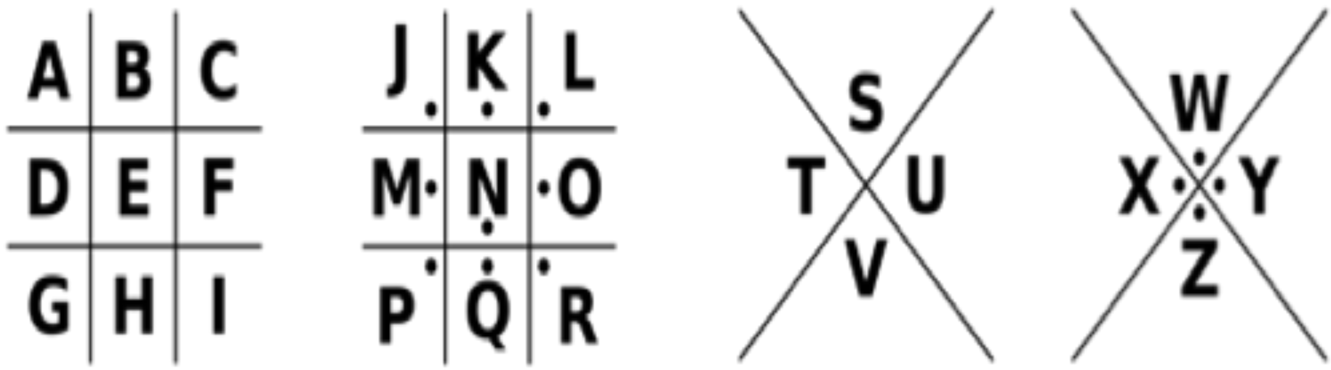
H	O	F	F	I	B	A
AABBB	ABBBA	AABAB	AABAB	ABAAA	AAAAB	AAAAA
C	O	N				
AAABA	ABBBA	ABBAB				

Neges gudd y tu mewn i neges arferol:
ES i i'r YsgoL HEdDiW, RoEdD hI'N BWRW GlAW AC YN WLyB Iawn YCh a Fi!

Twyll-len Cryptograffeg

Seiffr Pig Pen

Ysgrifennwch eich neges.
I amgryptio'r neges, anmewidiwch y symbol cyfatebol am pob llythyren
Y neges a anfonwyd yw'r casgliad o symbolau.
I ddadgryptio'r neges, anmewidiwch y symbolau gyda'r llythyren gyfatebol.



Enghraifft o Seiffr Pig Pen

Neges plaintext: Mae Cryptograffeg yn bwnc diddorol i astudio

Neges ciphertext:

technocamps

Twyll-len Cryptograffeg

Seiffr Shifft ac Enghraifft

Ysgrifennwch eich neges.
Dewiswch allwedd rhwng 0-25.
I amgryptio'ch neges, symudwch bob llythyren yn y neges ymlaen nifer yr allwedd o leoedd yn yr wyddor.
I ddadgryptio'r neges ciphertext, symudwch bob llythyren yn ôl nifer yr allwedd o leoedd yn yr wyddor.

Enghraifft:
Seiffr Caesar - Allwedd = 3

Neges Plaintext: Llyfr gwych ar cryptograffeg yw'r Llyfr Cod gan Simon Singh

Neges Ciphertext: Oobiu jzbfk du fubswrjudiihj bz'u Oobiu Frg jdq Vlprq Vlqjk

Allwedd = 16

Neges Plaintext: Mae cryptograffeg yn cael ei ddefnyddio drwy'r amser

Neges Ciphertext: Cqu shofjewhqvvuw od squb uy ttuvdottye thmo'h qciuh

Twyll-len Cryptograffeg

Seiffr Rail Fence ac Enghraifft

Dewiswch eich nifer o reiliau.
I amgryptio'ch neges, lluniwch grid ar gyfer y reiliau ac ysgrifennwch eich neges mewn patrwm igam-ogam ar hyd y reiliau.
Darllenwch y neges ciphertext ar hyd y reiliau, llinell wrth linell.
I ddadgryptio'r neges, crëwch grid gyda'r nifer cywir o reiliau a lleoedd ar gyfer y neges. Ysgrifennwch y neges ciphertext ar hyd y reiliau.

Nifer o reiliau: 5
Neges Plaintext: Gobeithio mwynhewch ein sesiwn
Neges Ciphertext: GOCIOIMWHSWBHWEEENETYHISINN
Dadgryptio: hyd y neges = 25, reiliau = 5
Yna ysgrifennwch y ciphertext ar hyd y reiliau, llinell wrth linell.

G								O								C								I		
	O						I		M						W		H						S		W	
		B				H				W				E				E				E				N
			E		T						Y		H						I		S					
				I								N								I						

G								O								C								I		
	O						I		M						W		H						S		W	

Twyll-len Cryptograffeg

Geiriau Allweddol

Steganograffeg
Cod
Amgryptio
Amnewid
Plaintext
Cryptograffeg
Seiffr
Dadgryptio
Trawsosod
Ciphertext

Steganograffeg - Yr arfer o guddio negeseuon neu wybodaeth mewn testun neu ddata nad yw'n gyfrinachol arall.

Cryptograffeg - Yw ymarfer ac astudio technegau ar gyfer cyfathrebu diogel.

Cod - Dull amgryptio lle mae geiriau neu ymadroddion cyfan yn y neges yn cael eu trosi'n rhywbeth arall.

Seiffr - Dull amgryptio sy'n newid neges ar lythyr fesul llythyr.

Amgryptio - Y broses o drosi gwybodaeth neu ddata i atal mynediad heb awdurdod.

Dadgryptio - Trosi data wedi'i amgryptio i'w ffurf wreiddiol.

Amnewid - Dull amgryptio lle mae llythrennau unigol yn cael eu rhoi yn lle llythrennau neu symbolau eraill.

Trawsosod - Dull amgryptio lle mae trefn y llythrennau yn y neges yn cael ei newid.

Plaintext - Y neges / testun gwreiddiol.

Ciphertext - Y neges / testun wedi'i amgryptio.