

UHOCTF (HARD)

Auteur(s) :

Hokanosekai, Senkei

Catégorie :

Crypto

Description :

Les membres du BDE ont développé un moyen de communication sécurisé, afin de pouvoir organiser des événements secrets. Cependant, lors d'une mission, un membre chargé de la communication a mis par erreur la totalité des emails universitaires dans la liste de diffusion. Voici le contenu du mail :

[mail.txt](#)

Flag UHOCTF{15/10/2025-23:30_AUGUSTE}

Solution

The screenshot shows a web-based interface for ADFGVX encryption. At the top, it says "CHIFFREMENT ADFGVX". Below that, a message in French reads: "★ MESSAGE CLAIR À CHIFFRER PAR ADFGVX ☹️ VOTRE COOPERATION EST ESSENTIELLE POUR PRESERVER LA NATURE CONFIDENTIELLE DE CETTE ANNONCE CORDIALEMENT L EQUIPE DU BUREAU DES ETUDIANTS UNIVERSITE DE LA ROCHELLE". The main part of the interface is a 6x6 grid of letters. The first row contains backslash, U, H, O, C, T, F. The second row contains U, G, P, X, A, L, F. The third row contains H, B, C, D, E, H, I. The fourth row contains O, J, K, M, N, O, Q. The fifth row contains C, R, S, T, U, V, W. The sixth row contains T, Y, Z, 0, 1, 2, 3. Below the grid, there are input fields for row and column indices, both set to 6, and an "OK" button. A "VIDER" button is also present. At the bottom, there is a text input field containing "GPXALFBCDEHIJKMNOQRSTUVWXYZ0123456789". Below this, it says "★ MOT-CLÉ (OU -> ORDRE DES COLONNES) POUR LA PERMUTATION CLE → (1,3,2) ⇔ (1,3,2)⁻¹". There is a checkbox for "★ COMPLÉTER LA DERNIÈRE LIGNE DES 'X' SI BESOIN" which is currently unchecked. A "CHIFFRER" button is at the bottom right. At the very bottom, it says "Voir aussi : Chiffre ADFGX".

COUHTFHUOCCOHCOCOOOOTOOUUOTTTUCOHOCCTCCFTCTTCCCHCHCCUCCUCCCTCTCCCCCCCUCUCT
TCCCTCCHCCCCHFCCCUCHHCCCCHOFOFCHUCCHOCCCUOCCCCCTCCCCCOFUCHOFCCOFCUUCTCC
CCTCTUFCCCFTTHHTTCUTFCCCHOCCHOTCTCCUCOCOCCTHCTTCCCHCOHHOHHCUCCHCUCUHOOHOHCHC
CHUHUCUHHCHOHUTUHCCCCCHHCCOHOOHOUCHHHOHCCOCHHUHTHUHUCHUHUUCHOCCCCCHHHUCOCUC
CCHHCOCOUOHHCUHHOUOOCUUCOHONHCCOHOHOOOOCCHOHUHHOHCCCCOHCOCCUUCHCCOCHUHHUH
CUOHCUOCOUCCCCCUCCHCHCHUHUCUOCOCCHCHCCCTOCHFCTCCCCCCCUCOFUFTFCCHTUUCCCOU
TTHFOHTUFCCCCOOHOFCCCCCTFTCCHTHHCTCCHOHOOHTCCTCUOHCCTCTTTHFHCCCUHFOFHCHHUC
HHFCCC000TCHFCTHHHC0OC0OHOOHHCTHHCCCCUCCCOCCOOTOCCCHTFCCCF0CCCOFOCCFOCHTH
CHCHCCHHHOHNHUHHCHNHUHHOHNHUHHUCCHHCHCHHHCCUCOOOHCCOCCUOCUUHCOOHOCCHCHCOUTCTT
TCOOUHCHCHOCCHOCSSCHONHTCHHHCUOOCCHCOUUCUOHCUHCCOCHUOHHCSSCOCHNOUOCHHOCCCHOC
HCCHUUOCCOHHCCHHUCHONCUHHNOHONHONHHCUHCHCOHHNHUHOHCUHCCHHNOCHCCOCOHCUHCCC
CCUUUOHHCOCUOUUHUHOOHUCHOCCOCHOCOUOCCOHHCCHCHOOTTHUHUUHHNHONHCHNOHCUUCOUOH
COCHOCSSCOHUCHHOCCOCHHHOHNOUHHHCCHONHCOOCHHOCOHCHONHNOHONHHHHUOUCCUUCOHONHHHC
OOHHUHUCHHHHHHOCSSCHUOHHTHOCSSCHOFHCHUHCCCTFCCOF00FCHHHCCCHCTCTHHOCCHHOCCFHC
TFTT0TCHF0CCCHUFHF0TTF0CTH0FTHCOC000UOCUCCOUCHCUCOFF0CCTHTOCUWHFTCTFTTHHC0
TEHOTCTC0CCTTCUCTCCHCCCHUTUTCOCOHOTHUCUUCCHCFCTC0CTCUCOOFHCUCCHCCFHUOCUTT

On va donc tester de décrypter avec un ADFGVX avec une table modifiée.

On peut voir la date : Le 12 juin 2023 à 22h donc --> 12/06/2023-22:00

Et le lieu de rendez-vous : PENTAKILL

Rechercher un outil

★ RECHERCHE SUR DCode PAR MOTS-CLÉS :

Tapez par exemple 'tirage au so

★ PARCOURIR LA [LISTE COMPLÈTE DES OUTILS](#)

Résultats

COUHTFHUOCCO...UTT

🔑 = 6,3,2,1,5,4

\	U	H	O	C	T	F
U	G	P	X	A	L	F
H	B	C	D	E	H	I
O	J	K	M	N	O	Q
C	R	S	T	U	V	W
T	Y	Z	0	1	2	3
F	4	5	6	7	8	9

CHERSMEMBRESDELUNITESECRETDEFENSECEMESSAGEEST
HAUTEMENTCONFIDENTIELETDITETRETRAITEAVECLAPL
USGRANDEDISCRETIONVEUILLEZNEPASDIVULGUERSONCO
NTENUADESTIERSNOUSVOUSINFORMONSDELORGANISATIO
NDUNEVENEMENTSECRETQUISETIENDRALE12JUN2023A2
2HAUPENTAKILLLACCESACETEVENEMENTESTSTRICTEMEN
TRESERVEAUXPERSONNESAYANTRECUCETTEINVITATIONN
OUSVOUSPRIONSDENEPARTAGERCESINFORMATIONSQUAVE
CLESPERSONNESDECONFIANCEEETDEVITERTOUTECOMMUNI
CATIONNONAUTORISEECONCERNANTCETEVENEMENTSECRE
TVOTRECOOPERATIONESTESSENTIELLEPOURPRESERVERL
ANATURECONFIDENTIELLEDECETTEANNONCECORDIALEME
NTLEQUIPEDUBUREAUDESETUDIANTSUNIVERSITEDELARO
CHELLE

DÉCHIFFREMENT ADFGVX

★ MESSAGE CHIFFRÉ PAR ADFGVX

UOHCTF{12/06/2023-22:00_PENTAKILL}

★ GRILLE CARRÉE DE CHIFFREMENT POUR LA SUBSTITUTION

\	U	H	O	C	T	F
U	G	P	X	A	L	F
H	B	C	D	E	H	I
O	J	K	M	N	O	Q
C	R	S	T	U	V	W
T	Y	Z	0	1	2	3
F	4	5	6	7	8	9

L GPXALFBCDEHIJKMNQIRSTUVWYZ0123456789

★ MOT-CLÉ (OU -> ORDRE DES COLONNES) POUR LA PERMUTATION

632154 → (6,3,2,1,5,4) ⇒ (4,3,2,6,5,1)⁻¹

► DÉCHIFFRER

SANS CONNAITRE LA CLÉ DE PERMUTATION

► ANALYSE DES BIGRAMMES

► BRUTE-FORCE DES PERMUTATIONS

SANS CONNAITRE LA GRILLE

► DÉSUBSTITUER

► Aller à : [Substitution Mono-alphabétique](#)

Flag : UOHCTF{12/06/2023-22:00_PENTAKILL}