

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

PROF

CHIFFREMENT ADFGVX

★ MESSAGE CLAIR À CHIFFRER PAR ADFGVX ?

VOTRE COOPÉRATION EST ESSENTIELLE POUR PRÉSERVER LA NATURE CONFIDENTIELLE DE CETTE ANNONCE

CORDIALEMENT

L ÉQUIPE DU BUREAU DES ÉTUDIANTS
UNIVERSITÉ DE LA ROCHELLE

\	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

6

×

6

OK

VIDER

L

GPXALFBCDEHIJKMNQIRSTUVWYZ0123456789

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

CLE → (1,3,2) ⇒ (1,3,2)⁻¹

★ COMPLÉTER LA DERNIÈRE LIGNE DES 'X' SI BESOIN ☐

► CHIFFRER

Voir aussi : Chiffre ADFGX

Subject: Réunion secrète [Gros Projet X A La Fac] - À ne pas divulguer

From: staff@bde.univ-lr.fr

To: universite-email-list@univ-lr.fr

Date: 09/06/2023 18:33:14

Message-ID: 632154

MIME-Version: 1.0

Content-Type: text/plain; charset="UTF-8"

COUHTFHUOCCOHCOCOCOCOTOOUUOTTTUCOHOCCTCCFTCTTCCHCCHCCUCCUCCTCTCCCCCCCUCU
CTTCCCTCCHCCCCHFCCCUCHHCCCCHOOCFCHCUCCHOCUUOCCCCCTCCCCOFUCHOFOCCOFCCUC
CTCCCCCTCTUFCCCFTTHHTTCUTFCCCHOCCHOTCTCCUCOCOCCTHCTTCCHCOHHOHHCUCHCUCUHOO
HOHCHCCHUHUCUHCHOHUTUHCCCHCCHHCCOHOHOUCHHHOHCCHCOHHUTHTUHUCHUHUCHOCCCCHC
HHUCOCUCCCHHCOCOCUOHHCUHOUOOCUUCOHOHHCCHOHOOUOOCCHOHUHHOHCCHCOHCOCUUUCH
CCOCHUHHUHCUCUOCUOCCCCCUCHCCHCHUHUCUOCOCCHCCTOCHFCFCTCCCCCCCUCUOFUFTF
CCHTUUCCCCOOUTTHFOHTUFOCOCOOHOFOCCTFTCCHTHHCTCCHOHOOHTCCTCUOHCCTCTTTHFH
CCCUHFOFHCHHUCHHFCCCOOTCHFCTHHHCOCOCOOHOOHHCTHHCCCCUCCCOCCOOTOCCCHTFCCC
FOCCCOFOCCFOCHTHCHCHCCHHHOHHUHHCHHUHHHHOHHUHHUCCHHCHCHHHCCUCOOHCCOCCUOCU
UHC00HOCHCHCOUTCTTTT00UHCHCHOCCHOCCHCOHTCHHHCUOOCCHCOUCCUOHCUHCCOCHUOH
HCCCOCHHOUCCHOCCHOCCHCHUUOCCOHHCHHUCHOHCUHHHOHOHHOHHHCUHCHCOHHHUHUHOHC
UHCCHHHOCHCCOCHCUHCCCCU00HHOCU0UHUHO0HUCHOCCOCHCOUOCCOHHCHHCHOOOTTU
HUUUHHHOHHCHHOHCUCUO0HHCOCHOCCHOCCHHOCCHHOCCHHOCCHHOCCHHOCCHHOCCHHOCCHHOC
HHOHOCHHHHHUOUCUUCOHOHHHC00HHUUCHHHHHHHOCCCHUOHHTHOCCCHOFHCHUHCCCTFCCO
FOFCHHHCHCTCTHHOCCHHOCCHHOCCHHOCCHHOCCHHOCCHHOCCHHOCCHHOCCHHOCCHHOCCHHOCCHHOC
CHCUCOFFOCCTHTOCUHFCTCTTTHHCOTFHOTCTCOCCTTCUCTCCHCCCHUTUTCOCOHOTHUCUCC
HFCFTCOCTCUCOOFHCUCHCCHFUCUTT

On remarque Gros Projet X A La Fac dans le sujet le nom bizarre, de plus on peut voir 632154 ce qui peut nous faire penser à un code de chiffrement ADFGVX. La composition semble contenir beaucoup de UOHCTF ce qui fait penser à une table de chiffrement modifiée.

PROF

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

CARRE DE POLYBE : UOHCTF et GPXALFBCDEHIJKMNOQRSTUVWXYZ0123456789
CLEF : 632154

On obtient :

CHERSMEMBRESDELUNITESECREDEFENSECEMESSAGEESTHAUTEMENTCONFIDENTIELETD
ETRETRAITEAVECLAPUSGRANDEDISCRETIONVEUILLEZNEPASDIVULGUERSONCONTENUADES
TIERSNOUSVOUSINFORMONSDELORGANISATIONDUNEVENEMENTSECREQUISETIENDRALE12J
UIN2023A22HAUPENTAKILLLACCESACETEVENEMENTESTSTRICTEMENTRESERVEAUXPERSONN
ESAYANTRECUCETTEINVITATIONNOUSVOUSPRIONSDENEPARTAGERCESINFORMATIONSQUAVE
CLES PERSONNESDECONFIANCEETDEVITER TOUTE COMMUNICATIONNONAUTORISEECONCERNAN
TCETEVENEMENTSECRETVOTRECOOPERATIONESTESSENTIELLEPOURPRESERVERLANATURECO
NFIDENTIELLEDECETTEANNONCECORDIALEMENTLEQUIPEDUBUREAUDESETUDIANTSUNIVERS
ITEDELAROCHELLE

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 D'CODE PAR MOTS-CLÉS :

Tapez par exemple 'tirage au so

★ PARCOURIR LA LISTE COMPLÈTE DES OUTILS

Résultats

COUHTFHUOCC...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

CHERSMEMBRESDELUNITESECRETFENSECEMESSAGEEST
HAUTEMENTCONFIDENTIELETDITETRETRAITEAVECLAPL
USGRANDEDISCRETIONVEUILLEZNEPASDIVULGUERSONCO
NTENUADESTIERSNOUSVOUSINFORMONSDELORGANISATIO
NDUNEVENEMENTSECRETQUISETIENDRALE12JUN2023A2
2HAUPENTAKILLACCESACETEVENEMENTESTRICTEMEN
TRESERVEAUXPERSONNESAYANTRECUCETTEINVITATIONN
OUSVOUSPRIONSDENEPARTAGERCESINFORMATIONSQUAVE
CLES PERSONNESDECONFIANCEEDEVITERTOUTECOMMUNI
CATIONNONAUTORISEECONCERNANTCETEVENEMENTSECRE
TVOTRECOOPERATIONESTESSENTIELLEPOURPRESERVERL
ANATURECONFIDENTIELLEDECETTEANNONCECORDIALEME
NTLEQUIPEDUBUREAUDES ETUDIANTSUNIVERSITEDELARO
CHELLE

DÉCHIFFREMENT ADFGVX

★ MESSAGE CHIFFRÉ PAR ADFGVX

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

6

×

6

OK

VIDER

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 : U0HCTF{12/06/2023-22:00_PENTAKILL}