Wyższa Szkoła Bankowa w Poznaniu Wydział Finansów i Bankowości Studia stacjonarne I stopnia – Informatyka

Sprawozdanie z wykonania Ćwiczenia laboratoryjnego

Przedmiot: Bezpieczeństwo i ochrona danych

Grupa: zlinz_3_6s_20/21_INF_Sp1_BiOD_gr.2

Prowadzący: dr inż. Izabela Janicka-Lipska

Ćwiczenie 01

Temat: Szyfry ADFGVX i Playfaira

Student: Patryk Kostrzewski

Data wykonania: 10.03.2021

1. Cel Ćwiczenia

Celem Ćwiczenia było zapoznanie się z architekturą i sposobem działania szyfru ADFGVX i szyfru Playfaira. Oraz przeprowadzenie i udokumentowanie eksperymentu polegającego na zaszyfrowaniu i odszyfrowaniu pliku w/w metodami szyfrowania.

2. Stosowane narzędzie

Ćwiczenie wykonano korzystając z aplikacji:

<u>CrypTool 1.4.41 — Polish version</u>

Dostępnej na stronie https://www.cryptool.org/en/ct1/downloads na licencji open source.

3. Stosowane algorytmy

3.1. Szyfr ADFGVX

Szyfr ten jest stosunkowo prostym aczkolwiek ciekawym szyfrem, który tworzy szyfrogram na podstawie macierzy. Za nagłówki kolumn i wierszy w macierzy przyjmuje się kolejno litery z nazwy szyfru (ADFGVX). Ów macierz posiada sześć kolumn i sześć wierszy wypełnionych 26. literami alfabetu łacińskiego oraz cyframi od 0 do 9. Znaki te wypełniają macierz w losowej kolejności, która jest znana tylko nadawcy i odbiorcy wiadomości.

Przykładowa macierz:

	Α	D	F	G	٧	X
Α	В	D	I	5	М	Т
D	N	L	0	W	F	Х
F	8	9	0	Α	4	7
G	U	R	J	K	Q	S
٧	С	Е	Р	3	2	1
X	Н	٧	G	Υ	6	Z

(Źródło: mattomatti.com)

Jednemu znaku jawnemu odpowiadają dwa znaki szyfrogramu w kolejności:

1 - nagłówek wiersza, 2 - nagłówek kolumny

Przykład:

Tekst do zaszyfrowania - PRZYKLAD

Znak jawny	Р	R	Z	Υ	K	L	Α	D
Znak zaszyfrowany	VF	GD	XX	XG	G	DD	FG	AD

Otrzymany tekst:

VFGDXXXGGGDDFGAD

Następnie wiadomość szyfruje się za pomocą klucza. Odbywa się to poprzez utworzenie macierzy, której nagłówkami kolumn są kolejne znaki klucza. Macierz wypełnia się wyżej uzyskanym tekstem szyfrogramu

Przykład:

Klucz szyfrujący - SZYFR

S	Z	Υ	F	R
V	F	G	D	X
X	X	G	G	G
D	D	F	G	Α
D				

(Źródło: własne)

W wypadku, gdy w macierzy zostaną puste pola (jak w powyższym przykładzie) można je wypełnić dowolnymi znakami lub konkretną literą np:

S	Z	Υ	F	R
V	F	G	D	X
X	X	G	G	G
D	D	F	G	Α
D	G	D	A	F

(Źródło: własne)

Ostatnim krokiem w procesie szyfrowania jest sortowanie kolumn alfabetycznie według nagłówków.

F	R	S	Υ	Z
D	X	V	G	F
G	G	Х	G	X
G	Α	D	F	D
А	F	D	D	G

Odczytując kolejno znaki z uzyskanej macierzy otrzymujemy szyfrogram:

DXVGFGGXGXGADFDAFDDG

Deszyfrowanie:

Aby odszyfrować wiadomość należy zapisać szyfrogram w formie tabelki i dokonać transpozycji kolumn zgodnie z kluczem a następnie odczytać znaki zgodnie z tabelką utworzoną na początku procesu szyfrowania.

3.2. Szyfr Playfair'a

Szyfrowanie tekstu jawnego za pomocą szyfru Playfair'a rozpoczynamy od utworzenia macierzy 5x5. W macierzy może znajdować się tylko 25 znaków. Więc z uwagi na fakt, iż alfabet łaciński posiada 26 znaków często przyjmuje się literę I oraz J jako jedność lub wyklucza się jedną z mniej używanych liter np. Q lub X.

Przy uzupełnianiu znaków w macierzy wykorzystujemy klucz szyfrujący z którego usuwamy powtarzające się znaki i rozpoczynamy wpisywanie znaków od ów klucza.

Drz	dela	ત ٠
P1 21	ykła	u.

Klucz szyfrujący:

GITARASZYFR

Powtórzenia w kluczu:

GITARASZYFR

Klucz szyfrujący po usunięciu powielających się liter:

GITARSZYF

Wypełnianie macierzy kluczem:

G	I	Т	Α	R
S	Z	Υ	F	

Pozostałe puste pola w macierzy uzupełnia się pozostałymi literami w kolejności alfabetycznej tak, aby uniknąć powtórzeń oraz przyjmują I i J jako jedną literę:

G	I	Т	Α	R
S	Z	Y	F	В
С	D	E	н	К
L	М	N	0	Р
Q	U	V	w	х

(Źródło: własne)

Następnym krokiem jest podzielenie tekstu jawnego na pary liter:

Tekst jawny:

WIADOMOSC

Podzielony na pary liter:

WI-AD-OM-OS-C

W przypadku, gdy tekst jawny ma nieparzystą ilość znaków aby uzyskać ostatnią parę zwykło się dopisywać jeden z rzadziej używanych symboli np. Q lub X

Finalnie podzielony tekst:

WI-AD-OM-OS-CX

Algorytm szyfrujący na podstawie par liter wyznacza prostokąty w utworzonej przez nas macierzy przyjmując za przeciwne wierzchołki parę podzielonego wcześniej tekstu jawnego. Następnie jako tekst szyfrogramu przedstawia pozostałe wierzchołki. Robi się to wedle zasad przyjętych przez nadawcę i odbiorcę wiadomości.

Przykład:

Pierwsza para (WI) - czerwony

Wyznaczony prostokąt - zielony

Pozostałe wierzchołki (UA) - pomarańczowy

G	ı	Т	А	R
S	Z	Υ	F	В
С	D	E	н	К
L	M	N	0	Р
Q	U	V	w	х

Operację powtarza się dla wszystkich par tekstu jawnego stosując uzgodnione wcześniej przez nadawcę i odbiorcę metody w przypadku powtórzeń w kolumnach lub wierszach.

4. Wykonane badania

4.1. Szyfr ADFGVX

Przy użyciu programu CrypTool zaszyfrowano przykładowy plik F-16.txt za pomocą macierzy standardowej, macierzy losowej oraz hasła zastępczego. Po szyfrowaniu każdą z metod sukcesywnie odszyfrowano plik również przy pomocy programu CrypTool.

4.2. Szyfr Playfair'a

Przy użyciu programu CrypTool zaszyfrowano przykładowy plik F-16.txt. Następnie również przy użyciu programu CrypTool odszyfrowano plik.

5. Uzyskane rezultaty

5.1. Szyfr ADFGVX

Plik F-16.txt (Bez liter spoza alfabetu i wielkimi literami na podstawie pliku eB-16.txt)

<mark>오</mark>류 F-16 PANNACZTERECHCHOPACHHXVIIIJIKWNGWWZNKPNBPSBJZSSRCDMSSFSWBBTJSLDSSBGFAPCGTAGGSASGWSBGZTSGNAOSGNFASW 7 A STWCTJBNTZCSWAGWBWWGGRWPWCIPWGGTMPNBUWONBGNBBICNDCGNPZMCPFTGWOOJWSPBAOWMLFGTSAFMGNWFCJNJKJFCR OGZTMTATAMNFGCPFBFGSJBTNCTTRGPJNMPZAGWFJAFSNNAGKOTFWGJGCAPNGZFPACWNNGZSSKZMBJWPTMBPZAFSWBAGWBBIGN 🤋 OJZGCTANZPRWA LIFDCRCOTWKCRWZKSOJRACWPWGGDWFTZGNWRPHNGTMRGDTTSPNPGNHZGPZPOGEOZTWCWSCSGTCFTJCPTRGN 🖫 ZOSSSNPOZFGLWFGNPMPNWSGSDGZCWRSPFTPFSOPNOFJSFKPJJJFBSATWJCFUCPZFGWNPNGNFGDSFGWTOTGPGGBZDTFZPJFTSP WRRZCJWFDFDKHGGKSFPLDGNKMFKPTOGJWFAWJAFMTBSNTSFSBMRCDFCHJUCAFNANNFSZKGCPAFJZGARFAPNFRANMPDWFGPNAP AGPWFPOGKAABPPAFFUPASGPPPKNDPSNAFNFIWWBSNJPWRKZZBTTNSPCCBFPBASWSNTJSATSAUSAJKJKJCICPBAPFAPTMSSJSFAP 🤉 GJFKAGSSGSFTWIGFMAKRAGWBDFSSSTRZSSZRARLACGMPNTJGFSOFGLFGDBTZAJTDPBFNGAFGZJGPKWFFTBMLTSCJAGPBSSFTWFP GJTSJGJEZSENENAPBNCBSGCWTSZTNESKSNDSGSANENGKMNMECBKTSEOMGNGEGEKJCJSCBMPNHPPEGCSWTGSKSEDBATPEATAPEM 🗵 NJMPSTICTSMANWDJAWSFDNASABBSWDPAFCRSFPPSTIPJTMDFZJMVNAFAWBHCKFCSPAFBLPKRSBAUMNKBJANABZMTPATSZFNPGMA FDPBGBTPWSZPMTWSCJSPPZJTPJDSAPDWGPDNJRCPUTKNGGAZBTBBJABDPBSAOFNSTFAJMABWAPOSCSSJSOZSPSTZWSWSFCZNOM p GSNNZWSTZDSZSWMSNFDPCTSAPGSAABTPAFNNSMGPACMCTPSAWMPRJCWDWSMOACRSNBFUGAMFSMJTNTSTPGPAMSJMFNACSMZ 🤉 JMPCJSUMUUMKDBSCNJASAMNZMMSCWSJOMTTMZMMUTHASBTSMSMNNCNSRZFMOMFJFPMSSJNCJSUMTFPNNZMJMSFPFBBNSNPWM 🛭 TWBWSZPESKWNSZMWWOFZWPKMWSWWBWTPEPWMWDKSMUPWSAWFTZCDWZPSGAFCWASNSWWPT.ITSPCRPWUZSPSNWASOTM 🖫 WRJAWAAPSTWSDPKSPSATTBWJWTSPWSCWTSBSMKLSPTDCWBPPKPSSPASJPSWCSMSNCPWTSTTPNSOWSSSSCDPWMSWWSPWK 3 SNMFWTPNPFRMSFSDOTBNRSRWCZSBWCFPSPBFWSSTTBBWFTFMCSMWFFNTNNSBFPNSZFRIFMAKGPMWSPPCOPGSTDFNMOSKGSU A NSMTGFPPJJCCGFNOGCPJCTSMPNTJCTNBGSTIDCWGTCSTWDJSTGTWMZFATWNFAIIDCTNIFSZASNAIFSWWFAKTSNAISAFWTZWNWRNPF EPPAII7EWOTNCJSMNDPPEPWSSPEMERSZWSPTZSPSSALWSTWAEPDTBPSPDBSANDTDAWEUPSEDTGSNTZENAJIZBSNZBASWNPSJWCP 🛭 TNBPEZESWEPSBRCMMEDBPBLABPENMSCEWSBBTMAMWKSETWEWSOCSBWTNMBDBEPSMEBSBCISMSAWAHEKKPPTTWSWSEMNNTTT 2 PBKRNNIKPFTWSZNTWAFWMWPTMATCPNMSMWFFSWAWKPFZWSJNTSWSFSNSTWMAPBZPFZNMKBNBABZNSSMTTWWJBWZAPBKBNS , FNAPSDCTFSGFSRPFKBSFWFWPNPDAPNFJNBSAPNNPSDDBKBFPBNBWFPCTDSJFATZPPJLPPWKPSONSSBKFODNDSSPSJADASTASWB 🕫 KWFNPPWTAINBIBKWSAFWLPFSZMFWFWFDNDKFTDJPSFNATGFPNSKBBTFTSFFCSFBOFSWFFTTTSMSFNBNMWTSWMBWSMZNWMLT WCGMCKTPWSPFSFWFSPSJSJFOKBKSATZRRWKSWFMKKSWMWPBTWWWLTKFSANPZJAKBBKBCPFMBNFNSGOWTZSGOMPABNGPAC KSSOMBFSWBNCBSBRZSRSPFBBWKTWFWWCFBSTTMPFNCNTACGFKBWNSAGNPTWIDPSSBCPOOGTMAMRMNKOAOBAACAJATIBACA

Zaszyfrowany plik przy pomocy macierzy standardowej i hasła transpozycji: SZYFR



Odszyfrowany tekst:

- - X 🚰 ADFGVX deszyfrowanie <ADFGVX szyfrowanie <F-16>, klucz <SZYFR, ABCDEFGHJKLMNOPQRSTUVWXYZ0123456789>>, klucz <SZYFR, ...> pannaczterechchopachhxviiijikwngwwznkpnbpsbjzssrcdmssfswbbtjsldssbgfapcgtaggsasgwsbgztsgnaosgnfaswstwctjbntzcswagwbwwggrwpwcipwggtm 🛭 🗸 pnbuwonbgnbbicndcgnpzmcpftgwoojwspbaowmlfgtsafmgnwfcjnjkjfcrogztmtatamnfgcpfbfgsjbtncttrgpjnmpzagwfjafsnnagkotfwgjgcapngzfpacwnngzsskzm 과 bjwptmbpzafswbagwbbignojzgctanzpbwajjfdcbcotwkcbwzksojbacwpwggdwftzgnwrphngtmbgdttspnpgnhzgpzpogfoztwcwscsgtcftjcptbgnzosssnpozfglwfg 🛭 npmpnwsgsdgzcwrspftpfsopnofjsfkpjjjfbsatwjcfucpzfgwnpngnfgdsfgwtotgpggbzdtfzpjftspwrrzcjwfdfdkhggksfpldgnkmfkptogjwfawjafmtbsntsfsbmrcdfchjuca 🛭 mannfszkgcpafizgarfapnfranmpdwfgpnapagpwfpogkaabppaffupasgpppkndpsnafnfiwwbsnjpwrkzzbttnspccbfpbaswsntjsatsausajkjkjcicpbapfaptmssjsfapgjf kagssgsftwigfmakragwbdfssstrzsszrarlacgmpntjgfsofglfgdbtzaitdpbfngafgzjgpkwfftbmltscjagpbssftwfpgjtsjgifzsfnfnapbncbsgcwtsztnfsksndsgsanfngkmn mfcbktsfomgngfgfkjöjscbmpnhppfgcswtgsksfdbatpfatapfmnjmpstictsmanwdjawsfdnasabbswdpaforsfppstipjtmdfzjmvnafawbhckfcspafblpkrsbaumnkbjana 🛭 bzmtpatszfnpgmafdpbgbtpwszpmtwscjsppzjtpjdsapdwgpdnjrcputknggazbtbbjabdpbsaofnstfajmabwaposcssjsozspstzwswsfcznomgsnnzwstzdszswmsn 🛭 fdpctsapgsaabtpafinismgpacmctpsawmprjcwdwsmoacisnbfugamfsmjtntstpgpamsjmfnacsmzjmpcjsumuumkdbscnjasamnzmmscwsjomttmzmmuthasbt 🛭 smanncnsrzfmontfipmssincjsumttpnnzmjmsfpfbbnsnpwmtwbwszpfskwnszmwwofzwpkmwswwbwtpfpwmwdksmupwsawftzcdwzpsgafcwasnswwptitsp crpwuzspsnwasotmwrjawaapstwsdpkspsattbwjwtspwscwtsbsmklsptdcwbppkpsspasjpswcsmsncpwtsttpnsowsssscdpwmswwspwksnmfwtpnpfrmsfsdot 🛭 brirsrwczsbwcfpspbfwssttbbwftfmcsmwffintnnsbfpnszfrifmakgpmwsppcopgstdfnmoskgsunsmtgfppjjccgfnogcpjctsmpntjctnbgstidcwgtcstwdjstgtwmzfatwn⊋ faiidctnifszasnaifswwfaktsnaisafwtzwnwrnpffppaiizfwotncjsmndppfpwsspfmfbszwsptzspssalwstwafpdtbpspdbsandtdawfupsfdtgsntzfnajizbsnzbaswnpsjw 🛭 cptnbpfzfswfpsbrcmmfdbpblabpfnmscfwsbbtmamwksftwfwsocsbwtnmbdbfpsmfbsbcismsawahfkkppttwswsfmnntttpbkrnnikpftwszntwafwmwptmatcpnms 🛭 nwffswawkpfzwsintswsfsnstwmapbzpfznmkbnbabznssmttwwjbwzapbkbnsfnapsdctfsqfsrpfkbsfwfwpnpdapnfjnbsapnnpsddbkbfpbnbwfpctdsjfatzppjlppwk psonssbkfodndsspsjadastaswbkwfnppwtainbibkwsafwlpfszmfwfwfdndkftdjpsfnatgfpnskbbtftsfffcsfbofswfftttsmsfnbnmwtswmbwsmznwmltwcgmcktpwspfs ب wfspsjsjfokbksatzrwkswfmkkswmwpbtwwwltkfsanpzjakbbkbcpfmbnfnsgowtzsgompabngpackssombfswbncbsbrzsrspfbbwktwfwwcfbsttmpfncntacgfikbw a nsagnptwidpssbcpoogtmamrmnkoaaobaacajatibacaomnwwcwfiarmwjitawptwpupfswobwtsjbmsziptnntabwpsbmacwnnswaomnwsawstrwawsspsabsnwsa 🛭 daplwdcnwwsosanapdsatwswtfwwtfrcskzpmbdnnswpbpaipwfanpopppbbaspspfrftufckszpfwsstpusbasazsfabbsnfpnstmpsdtpftwbsnrzskzwtjwsapatpawwl 🛭 tnuspiwnsofswykmatymwoybkakisubtpwztzagomnossonaisawuwysslwazszntadsfsmzmzwyiszrknsfpontfsobtsctwftonykaiimzkstwkdbcnrunzosdkid 🛭 wzscgpsaannndacbastdpokbwrsbkrtgwapmswnkcgptkskdsjfkstwktwssjbssbbdftngsfsmbkpgzsassazbzbcanappgnhbwtcfjbangjscnbsnfrtpcdzrdtdksgno 🗟 swufddmfdngdgsfdawsspadcsdnsbpsnjzsnwsbwddskacfnsctcascoejukmuskcnmnhjcbzktkcztbfasjssmcakfbsanjdsdnjpmfrsbbokznfsjsskbkskmbwijwkd 🛭 snskswbjptsotbdbrntbskubkstsknsmzkupgjcbnacpspgzaskbwppgbscgtsjwrpccwasnbpsdtwbatwsttmwszbwdwsncpnmtpnsspfzwmnjtngstbjkwnnsjsssn 7

Zaszyfrowany plik przy pomocy macierzy losowej i hasła transpozycji: SZYFR



Zaszyfrowany plik przy pomocy hasła zastępczego i hasła transpozycji: SZYFR

ርå ADFGVX szyfrowanie <F-16>, klucz <SZYFR, GITARSEMBCDFHJKLNOPOUVWXYZ0123456789> - - X GADAGFAFXADGAVFDXVXDXAFFGAAGAAXAXVXAXDXAGDFAGDVAAAVAAGXAFDVFDGFFDGGDXAXFXFFDXAFAVDXADFFADGGDGFGFXFGF 7 A DAVAXVFGDVXDADAFAADGDDFAFGFFGGAGFFVFFAFGAFAGAVVAXDFGFVXFXAVFDGAAGAXDXFDFDDXGGDDGAFADVAADVVDAVVDDVAF 7 GVFXAADVDFFXDVDADXFXFGDDAGDGGVGGAVFFDADAAAFAAVGFFVVFFADAAXFGAXFFAAGGDXDADGAXGAAVGVAFADAGDVAXAXDDAAF 7 GVAGXDFFAAXDAAAVXFADXGXFXFXAXFVDFDDAAFDDAGXAFFXAAAAFDAGDVFVDGDXGXAAAADXDVAFFGAFFXGVFVVFADGDDFAVGFDXVF DGGAFGAVAFDGGXDXADGADXFXAVAGFAFVVXGXDGAAAFDVAGDAGADVDGAFADDFAAAXDGDDDXGDDGAGVDGDADDFAFAVFVDDDDFGG 🕫 FFDDXDVGDDXDFADFDFVGVDVDXGXDDGAAGAXGDGVGXFGAVAGAVGXAFFFGGAXFADFFXADGXFAAFAVAGGXAVFXGADXFFAVAVGAGXDV 7 DGGXFXGXAXFAAAGXDDFXAFGDDXAAADAGDXDVDFFFGDAVAVFXAVDVAFAXGDGVDAAXAGDVDVGDAVAXAGAGDFGFFGFDFFDADADAVF 7 GFADVAVDVDGDDDXAGFXDXAVDVGDAGDGFFGFGXFFDVAAGDGXGFAAAVAGGDFFAXADDAFFDFADGDVADXAXAXAADXGVAVFXFADFGVDG AXVAGVAVDXFXAGAGDVGVAFFXGAVXGVFFGXAXAFDXDXFXDFDXFVGFDVFVDFGADXAXFFADGXDFDAGVFXGDDFGDDXGDFAFAFXDXFFAXG FFVGXADFVDXGXFFDXDXAGDFAFDDAGFVDXAVAVGFAXADADFFGXAVAGFXAVGXAXAVFVGXAGAFGXAVFADVGAGXGADGAXAXAAAFAGVXD 7 VFFAFAFAXGDAGAVFXGXAVAVAFFXAVVGDAGGAFAGVDAXDDGXFXFFGFAXFFADAFDVVXFVDAAVAFAADVFFADFGAXAXAFADAFAAAFAXA 🛭 DDGGADFFGFGAXGVDVAXGVDVAXGXDXAAFXAVAGFGAGFFAGFDVFVFAXDFAVAVDVDFDDFFDVGVAXFFAVFFGFAVVFFFDXVXGAAAFVDG 🛭 DXGGAFAFGVFFAAGVEXEVAXFFAADEDXGFDAAGEVAVAFGXVVEXEGAXEVAGAXAFAGADDVGGFFDXFFFVEXDAAFDGVFAXEXAGAXDVAVAXV 🗵 XAAAGADDGGXDFFVFFAADVAXVGVADXAXGXDDAGDVFAAVDDGVDFDXDFFFFVADAVGVAVFAAFFAGDFXGDGVADAXDFAFGVAFAGFXDVDF 🕫 GDGXFVGVDVFDGVAXGDAXVGFADFDGDDGADGFXVVGXGXGFVADXAGDAFXDFGDDGFXVGVFAGGDFDAXGDDXDVDFAFDDADDVGAGVGADD GGFAGDDFFFFFFDXDADDAGDGADADGFDGGFDFAXGVVGGDFVAGGXDXFVDFAFDXAVGVDDAFDFGXDFAFGAVFAAAGDAVGDGFDDAVAXD ; DDXDAAAAADDAGAXGFAFVXAFAVGDAFFFFADGDVDAAXGAFDAXDVDVFGAFAGDGDADVAAFAAXDVAXGDAVDGFAADFADDAFGFFDDGGVF 🤉 vdfdvaddaavvvgvdaaaaagadddxagfaadavvadvgvaagxaxgxaffxavdgdvfvdxafafaddxadgvfaaaaffffxfxdvdfdxfgfvaf 🔋 GXAVGXFADAGADXAFAXAAGVAGDVADADAVDFDXFDAGAFFDDAGDFXAXAXDVDGAVDXAXAVDDAAFAAFAFDVDDGVADADGXAXFXADFVDGA 🛭 VVVFVAGFFDGAXAADDAFFAAXAFDGDFDVGFADGDAVAFGADXGFFDVDAGFFAGFFDFFDADGFDAAVAFAAGGGDGVGVDDGFAGAFDAAXAG AVFGFXGFAXVXAVADVVFVAGAGGXAADGAVAGGDDXDADDFXAGFXDDDGGFFFFGDDAVFFVDFXAXFVVDDXADFFDVDDGFAAAFVXGXGXGFA vaxdvdaaxdvaggxgaaagfgvafagaxaaggddavgxdgaggfaggvdvgxgxaxdvgxfvgaddaxfxdxdadvafdxavfvdavvdfdxdaaxff GXAAFGFAFFGFAFAVAGGDAVDFDDDVAGAXGGAGAVGVGXADGFFDGXAADXAFGXGFDVGAAVDVGXAVDGVXDXGDGVDXDXDDDFDXAXDFDF 7

Odszyfrowany tekst:

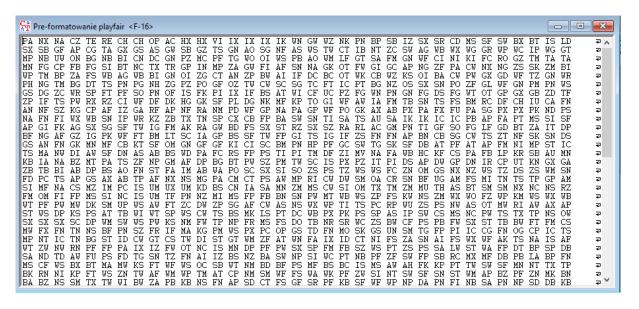
🚰 ADFGVX deszyfrowanie <ADFGVX szyfrowanie <F-16>, klucz <SZYFR, GITARSEMBCDFHJKLNOPQUVWXYZ0123456789>>, klucz <SZYFR, ...> pannaczterechchopachhxviiijikwngwwznkpnbpsbjzssrcdmssfswbtjsldssbgfapcgtaggsasgwsbgztsgnaosgnfaswstwctjbntzcswagwbwwggrwpwcipwggtm 🛭 🗸 pnbuwonbgnbbicndcgnpzmcpftgwoojwspbaowmlfgtsafmgnwfcjnjkjfcrogztmtatamnfgcpfbfgsjbtncttrgpjnmpzagwfjafsnnagkotfwgjgcapngzfpacwnngzsskzm a bjwptmbpzafswbagwbbignojzgctanzpbwajjfdcbcotwkcbwzksojbacwpwggdwftzgnwrphngtmbgdttspnpgnhzgpzpogfoztwcwscsgtcftjcptbgnzosssnpozfglwfg a npmpnwsgsdgzcwrspftpfsopnofisfkpjjjfbsatwicfucpzfgwnpngnfgdsfgwtotgpggbzdtfzpjftspwrrzcjwfdfdkhggksfpldgnkmfkptogjwfawjafmtbsntsfsbmrcdfchjuca 🛭 fnannfszkgcpafizgarfapnfranmpdwfgpnapagpwfpogkaabppaffupasgpppkndpsnafnfiwwbsnjpwrkzzbttnspccbfpbaswsntjsatsausajkjkjcicpbapfaptmssjsfapgjf 🕫 kagssgsftwigfmakragwbdfssstrzsszrarlacgmpntjgfsofglfgdbtzajtdpbfngafgzjgpkwfftbmltscjagpbssftwfpgjtsjgifzsfnfnapbncbsgcwtsztnfsksndsgsanfngkmn 🔻 mfcbktsfomgngfgfkjcjscbmpnhppfgcswtgsksfdbatpfatapfmnjmpstictsmanwdjawsfdnasabbswdpafcrsfppstipjtmdfzjmvnafawbhckfcspafblpkrsbaumnkbjana 🔻 bzmtpatszfnpgmafdpbgbtpwszpmtwscjsppzjtpjdsapdwgpdnjrcputknggazbtbbjabdpbsaofnstfajmabwaposcssjsozspstzwswsfcznomgsnnzwstzdszswmsn a fdpctsapgsaabtpafnnsmgpacmctpsawmprjcwdwsmoacisnbfugamfsmjtntstpgpamsjmfnacsmzjmpcjsumuumkdbscnjasamnzmmscwsjomttmzmmuthasbt 🕫 smsmnncnsrzfmomfjfpmssjncjsumtfpnnzmjmsfpfbbnsnpwmtwbwszpfskwnszmwwofzwpkmwswwbwtpfpwmwdksmupwsawftzcdwzpsgafcwasnswwptjtsp 🗟 crpwuzspsnwasotmwrjawaapstwsdpkspsattbwjwtspwscwtsbsmklsptdcwbppkpsspasjpswcsmsncpwtsttpnsowsssscdpwmswwspwksnmfwtpnpfrmsfsdot $\overline{\iota}$ bnrsrwczsbwcfpspbfwssttbbwftfmcsmwffntnnsbfpnszfrifmakgpmwsppcopgstdfmmoskgsunsmtgfppjjccgfnogcpjctsmpntjctnbgstidcwgtcstwdjstgtwmzfatwn 🛭 faiidctnifszasnaifswwfaktsnaisafwtzwnwrnpffppaiizfwotncjsmndppfpwsspfmfbszwsptzspssalwstwafpdtbpspdbsandtdawfupsfdtgsntzfnajizbsnzbaswnpsjw 🔻 cptnbpfzfswfpsbrcmmfdbpblabpfnmscfwsbbtmamwksftwfwsocsbwtnmbdbfpsmfbsbcismsawahfkkppttwswsfmnntttpbkrnnikpftwszntwafwmwptmatcpnms a mwffswawkpfzwsjntswsfsnstwmapbzpfznmkbnbabznssmttwwjbwzapbkbnsfnapsdctfsqfsrpfkbsfwfwpnpdapnfjnbsapnnpsddbkbfpbnbwfpctdsjfatzppjlppwk 📮 psonssbkfodndsspsjadastaswbkwfnppwtainbibkwsafwlpfszmfwfwfdndkftdjpsfnatgfpnskbbtftsfffcsfbofswfftttsmsfnbnmwtswmbwsmznwmltwcgmcktpwspfs 🗟 wfspsjsjfokbksatzrrwkswfmkkswmwpbtwwwltkfsanpzjakbbkbcpfmbnfnsgowtzsgompabngpackssombfswbncbsbrzsrspfbbwktwfwwcfbsttmpfncntacgfkbw 🔻 nsagnptwidpssbcpoogtmamrmnkoaaobaacajatibacaomnwwcwfiarmwjitawptwpupfswobwtsjbmsziptnntabwpsbmacwnnswaomnwsawstrwawsspsabsnwsa 🕫 dapiwdcnwwsosanapdsatwswtfwwtfrcskzpmbdnnswpbpaipwfanpopppbbaspspfrftufckszpfwsstpusbasazsfabbsnfpnstmpsdtpftwbsnrzskzwtjwsapatpawwl a tnuspjwnsgfswwkmatwmwgwbkakjsubtpwztzaagomnpsspnajsawuwwsslwazszntadsfsmzmzwwjszrknsfpontfspbtsctwftpnwkajimzkstwkdbcnrunzgsdkjd a wzscgpsaannndacbastdpokbwrsbkrtgwapmswnkcgptkskdsjfkstwktwssjbssbbdftngsfsmbkpgzsassazbzbcanappgnhbwtcfjbangjscnbsnfrtpcdzrdtdksgno 🛭 swufddmfdngdgsfdawsspadcsdnsbpsnjzsnwsbwddskacfnsctcascoejukmuskcnmnhjcbzktkcztbfasjssmcakfbsanjdsdnjpmfrsbbokznfsjsskbkskmbwijwkd 🛭 snskswbjptsotbdbmtbskubkstsknsmzkupgjcbnacpspgzaskbwppgbscgtsjwrpccwasnbpsdtwbatwsttmwszbwdwsncpnmtpnsspfzwmnjtngstbjkwnnsjsssn 🛭 🕹

5.2. Szyfr Playfair'a

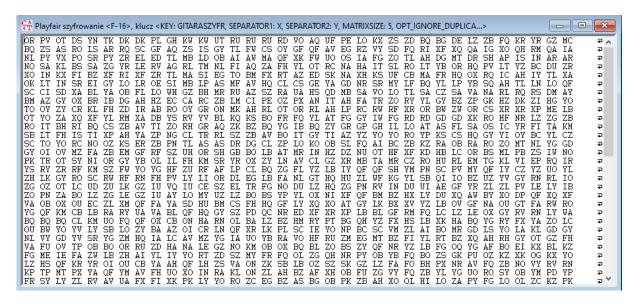
Plik F-16.txt (Bez liter spoza alfabetu i wielkimi literami na podstawie pliku eB-16.txt)



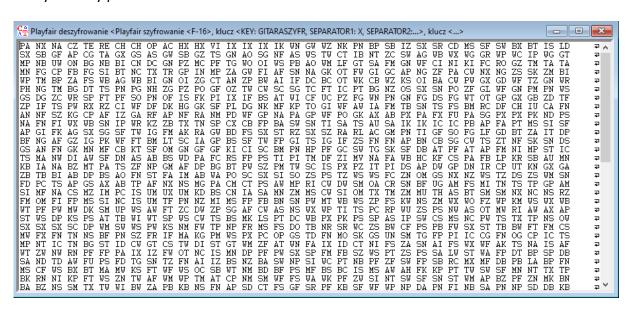
Podzielony na pary i przygotowany do szyfrowania plik;



Zaszyfrowany plik przy pomocy klucza GITARASZYFR



Odszyfrowany plik:



6. Wnioski

6.1. Szyfr ADFGVX

Szyfr ADFGVX w moim odczuciu wydaje się być szyfrem stosunkowo prostym w implementacji. Zasady jego działania są bardzo czytelne i nawet ręczne szyfrowanie i odszyfrowywanie nie powinno sprawiać dużych problemów.

Jednocześnie ciężko mi ocenić jak bardzo jest on bezpieczny w obliczu mocy obliczeniowej dzisiejszych komputerów.

Jako jego dość sporą wadę uznaje konieczność znajomości nie tylko klucza szyfrującego ale i również macierzy, która tworzy się na początku procesu szyfrowania w celu przypisania do

niej odpowiednich znaków. Przy macierzy standardowej szyfr zdaje się być dużo prostszy do złamania. Natomiast przy macierzy losowej konieczność posiadania jej wraz z kluczem znacząco może utrudnić przekazanie wiadomości i jej ręczne odszyfrowywanie bez komputera.

6.2. Szyfr Playfair'a

Szyfr PLayfair'a również jest stosunkowo prostym w implementacji szyfrem, który łatwo stosować ręcznie. Jego implementacja w moim odczuciu wydaje się być prostsza niż implementacja szyfru ADFGVX.

Jeśli nadawca i odbiorca często komunikuję się za pomocą ów szyfru i mają swoje ustawione reguły dot. odczytywania szyfrogramu cały proces powinien przebiegać sprawnie. Natomiast jeśli wiadomość będzie odszyfrowywana w błędny sposób rezultatem będzie znacznie większy nakład pracy.

W tym wypadku również ciężko mi określić poziom bezpieczeństwa tego szyfru w obliczu dzisiejszej mocy obliczeniowej.

7. Literatura

- [1] Artykuł "Szyfry ADFGX i ADFGVX" https://mattomatti.com/pl/a35aj
- [2] Artykuł "Szyfr Playfair'a" http://www.crypto-it.net/pl/proste/szyfr-playfair.html