Projekt číslo 1.
Předmět A0M32IBE - Informační bezpečnost

Zimní semestr 2011

Bc. Jáchym Šimák
dne: 13.4.2011
skupina: Středa – 9:15

Obsah

Zadání

Zadání č. 314

Jméno: Šimák Jáchym (101)

Datum zadání: 02.03.2011

Datum odevzdání: 4.5.2011 23:55 CEST

Otevřený text je v anglickém jazyce. Před šifrováním byly z OT odstraněny mezery, interpunkce a čísla. K zašifrování byly použity jednoduché metody probírané na cvičeních:

- afinní šifra
- substituce s klíčem
- Vigenérova šifra
- transpozice s pevnou délkou periody
- úplná tabulka
- úplná tabulka s heslem
- dvojnásobná tabulka
- kombinace substituce a transpozice

Náležitosti závěrečné zprávy:

- zprávu odevzdejte přes Moodle (příslušný formulář najdete u 12. cvičení).
- zprávu odevzdejte ve formátu PDF
- jméno souboru zvolte podle vzoru KODPREDMETU__LS2011_QQQ_PRIJMENI.PDF, kde QQQ je číslo paralelky např. A0M32IBE_104_NOVAK.PDF

Závěrečná zpráva musí obsahovat:

- rozluštěný OT z jednotlivých podúloh
- informaci o tom, jak byly jednotlivé úlohy zašifrovány (tj.

typ šifry a její parametry)

- stručný postup, jak jste postupovali během kryptoanalýzy (pokud jste pro dešifrování použili jiné nástroje, než byly používány na cvičení, uveďte jaké, včetně internetových odkazů - tam, kde to je možné)

Hodnocení projektu:

- Maximální počet bodů, který lze za projekt získat - 50 bodů
- 40 bodů lze získat za vyluštění úloh
- 10 bodů lze získat za vypracování závěrečné zprávy (vzhled, originalita, formální požadavky, ...)

Úlohy jsou ohodnoceny následovně:

- Úloha 1 - 2 body
- Úloha 2 - 3 body
- Úloha 3 - 4 bodů
- Úloha 4 - 3 body
- Úloha 5 - 4 body
- Úloha 6 - 6 bodů
- Úloha 7 - 4 bodů
- Úloha 8 - 7 bodů
- Úloha 9 - 7 bodů

Pro vyřešení úloh můžete používat veškeré nástroje, které si naprogramujete, nebo vyhledáte na Internetu. Protože cvičící neznají řešení jednotlivých úloh, některé způsoby kryptoanalýzy (korupční, pendreková, social engineering), o kterých jsem mluvil na přednáškách, nepovedou k cíli.

Luštění zdar!
Tomáš Vaněk

Postup řešení

Útok na systém

Po několika rozluštěných textech se mi podařilo přijít, že mé zprávy jsou z pohádky St. George of Merrie England od Arthura Rackhama (viz literatura). Toto mi velmi usnadnilo následující luštění.

Úloha 1:

Zadání

CKZGNFCKTOBQETGEJBXMTPZBXHKZTMCKZTESTGJZETPTFGTGEHLBCZCKZUFZMDEMTP
BGXGEZMBGZBUKFHUQTLFGPNFGPHHBCKTCCKZNZTWBGWFZMJZECKZKZTMCTGETQQCKZ
PMTHHTMBXGECXMGZEJMFLHBGNFCKCKZOQBBECKTCUQBNZEUMBLCKZEDFGPLBGHCZM

Postup

Zde jsem provedl frekvenční analýzu a z výsledků jsem odtušil, že byla provedena substituce (text neseděl na angličtinu). Pustil jsem na ní C++ program, který jsem vytvořil na cvičení. Ten vygeneruje všechny možnosti (útok hrubou silou) a pomocí linuxovského příkazu GREP, jsem si nechal vypsat pouze ty řetězce co obsahovali string THE. Vyšli mi 3 možnosti v nichž jsem našel jednu obsahující smysluplný text.

Program

```
#include <iostream>
#include <string>
using namespace std;

int main () { string s1;
s1="CKZGNFCKTOBQETGEJBXMTPZBXHKZTMCKZTESTGJZETPTFGTGEHLBCZCKZUFZMDEMTPBGX
GEZMBGZBUKFHUQTLFGPNFGPHHBCKTCCKZNZTWBGWFZMJZECKZKZTMCTGETQQCKZPMTHHTM
BXGECXMGZEJMFLHBGNFCKCKZOQBBECKTCUQBNZEUMBLCKZEDFGPLBGHCZM";
cout << "lustime: " << s1 << endl;
for (int a=0;a<26;a++) {
        for (int b=0;b<26;b++)      {
                for (int i=0;i<s1.length();i++)
                        if (s1[i]==' ')  cout << " ";
```

```
                        else cout << (char)(  (( ((((int)s1[i]-65)+26-b )%26 ) *a )%26) +65) ;
                cout << "\ta=" << a << "\tb=" << b  << endl;             } }
  return 0; }
```

Zkompilovano g++ c.cpp -o c

```
xsimi@Holly:~/Fra$ ./c|grep THE
THENWITHABOLDANDCOURAGEOUSHEARTHEADVANCEDAGAINANDSMOTETHEFIERYDRAGONUND
ERONEOFHISFLAMINGWINGSSOTHATTHEWEAPONPIERCEDTHEHEARTANDALLTHEGRASSAROUNDT
URNEDCRIMSONWITHTHEBLOODTHATFLOWEDFROMTHEDYINGMONSTER          a=5       b=19
HBGRCIHBELYDZERZSYOTEUGYOABGETHBGEZVERSGZEUEIRERZAKYHGHBGNIGTQZTEUYRORZGT
YRGYNBIANDEKIRUCIRUAAYHBEHHBGCGEFYRFIGTSGZHBGBGETHERZEDDHBGUTEAAETYORZHO
TRGZSTIKAYRCIHBHBGLDYYZHBEHNDYCGZNTYKHBGZQIRUKYRAHGT   a=9       b=7
WMDEFPWMRUHYAREAXHZQRJDHZTMDRQWMDRACREXDARJRPEREATBHWDWMDGPDQLAQRJHEZ
EADQHEDHGMPTGYRBPEJFPEJTTHWMRWWMDFDRKHEKPDQXDAWMDMDRQWREARYYWMDJQRTT
RQHZEAWZQEDAXQPBTHEFPWMWMDUYHHAWMRWGYHFDAGQHBWMDALPEJBHETWDQ
          a=15      b=4
```

Zjištěný tip šifry

Affiní šifra A=5 , B=19.

Řešení

THEN WITH A BOLD AND COURAGE OUS HEAR THE ADVANCED AGAIN AND SMOTE THE FIERY DRAGON UNDER ONE OF HIS FLAMING WINGS SO THAT THE WEAPON PIERCED THE HEART AND ALL THE GRASS AROUND TURNED CRIMSON WITH THE BLOOD THAT FLOWED FROM THE DYING MONSTER

Úloha 2:

Zadání

```
QLQSBILPBILNIKBHDKWRTSLNNSCIWPIDWNTHCIDWDKWCDKBEKBESLKDQCDNSLNCEQQ
MIDPVCERCDSSCIAIBEKKEKBLNSCIRLJADSCDWQCEUIPIWDBDEKQSSCIAIDQSQQRDHY
ADRGCIJLTKSIWCEQQSIIWADYDPWDKWMPLRIIWIWSLSCIMDHDRILNSCIGEKBKLVSCIG
EKBQKDJIVDQMSLHIJYDKWVCIKCIQDVSCDSSCIWPIDWIWWPDBLKVDQEKWIIWQHDEKCI
BDUILPWIPQNLPSCIRESYSLAIWIRLPDSIW
```

Postup

Zde jsem provedl frekvenční analýzu a z výsledků jsem odtušil, že byla provedena substituce (text neseděl na angličtinu). Pustil jsem na ní C++ program, který jsem vytvořil na cvičení.

Ten vygeneruje včechny možnosti (útok hrubou silou), bohužel ani jeden nedal smysluplný text. V této chvíli jsem měl vyluštěné úlohy 1, 3, 4, a 5. V zadání zatím šli šifry pěkně postupně, zkusil jsem tedy zda to není kompletní substituce. Tyto informaci a znalost ukrytého textu (viz bod útok na systém), mi umožnily velmi rychle zjistit parametry šifry.

Zjištěný tip šifry

Kompletní substituce.

A → B	B → G	C → H	D → A	E → I	G → K	H → L
I → E	J → M	K → N	L → O	M → P	N → F	P → R
Q → S	R → C	S → T	T → U	U → V	V → W	W → D
Y → Y						

Řešení

so st george of england cut off the dreadful head and hanging it on a shaft of his spear which at the beginning of the combat had shivered against the beasts scaly back he mounted his steed bayard and proceeded to the palace of the king now the kings name was ptolemy and when he saw that the dreaded dragon was indeed slain he gave orders for the city to be decorated

Úloha 3:

Zadání

DROAEVIYMAJSWWEQGSTRLSEPIWLHAEHPDHFHFZGYDROVUVLTHNVSQLIOOEHBUMYZSW
KPHRJIEHTKIATLDGPTNGGZFMDROXDDLFGDUIOGOEPPLDUIDLEGMYVRLQDHNYIWOEWE
YWMRYYMEGSYFIOOHAIWIDMEHHDKIFLWRCDTLKIVSYXDWSPLCRVEAIPXSBTKICPIWLL
ELKSYHRZLTEEPYDBCLEYLWDPVXDEIQHRHEYWAIXPKFLPWBNJXSXALVHBTKWHXEWIDM
SRYYWS

Postup

Frekvenční analýza neseděla na anglický text. Na řadě Vigenerova šifra a po půl dne zkoušení nalezena správná kombinace.

Zjištěný tip šifry

periodicky posun o 5 znacích, posuny jsou 23,22,15,7,0 → Vigenérova šifra - periodické heslo: YXQIA

Řešení

AND HE SENT A GOLDEN CHARIOT WITH WHEELS OF EBONY AND CUSHIONS OF SILK TO BRINGST GEORGE TO THE PALACE AND COMMANDED A HUNDRED NOBLES DRESSED IN CRIMSON VELVET AND MOUNTED ON MILK WHITES TEEDS RICHLY CAPARISONED TO ESCORT HIM THITHER WITH ALL HONOR WHILE MUSICIANS WALKED BEFORE AND AFTER FILLING THEAIR WITH SWEETEST SOUNDS

Úloha 4:

Zadání

NWTOHBEEATIUFLSUAIABHRSEEFWLAHESDNDADESRSDTEHWEEAYKRNGHITWOSUDSNAD GNAEHVIINMSGNIOBEFTOTRHLAADAMIODRNIGONFURPETWSAERTxxxx

Postup

Jako první jsem si všiml podivných malých písmen x na konci textu. Zkusil jsem tedy transpoziční šifry. Podle pořadí v zadání vycházela transpozice s pevnou délkou periody. Ze zarovnání a x znaků vycházely možnosti 5,6 a 8 znaků. Podařilo se mi na začátku poznat slova NOW a THE a pak už to bylo celkem jednoduché.

Zjištěný tip šifry

Transpozice s pevnou délkou periody. Perioda 8 znaků.

Přepis který znak na který

1. → 1.
2. → 3.
3. → 4.
4. → 2.
5. → 5.
6. → 7.

7. → 8.
8. → 6.

Řešení

NOW THE BEATIFUL SABIA HER SELF WASHED AND DRESSED THE WEARY KHIGHTS WOUNDS AND GAWE HIM IN SIGN OF BETROTHAL A DIAMOND RING OF PUREST WATER

Úloha 5:

Zadání

TDBTSANSTIBANSOHBYHONITONEFYLLEETEFDFEREARLEDNEHGKHIDESUOUEEANEONA
CHSSTMLPNFIKLIDEETWIHLWLTNIDGBNRHHFEEIUEVNEHETEIIURDTTREGNTELTSLLB
HHEHSWSHNYIWESAIH**X**ETIPOMFRETALME**X**HETUOAEEAHBCTR**X**ADHRDGADREIOOG**X**

Postup

Všiml jsem si znaků x umístěných ke konci textu s offsetem 15. Zkusil jsem tedy tabulku o rozměrech 13x15 a bylo hotovo.

Zjištěný tip šifry

transpozice - úplná tabulka 13x15

Řešení

Then, after he had been invested by the King with the golden spurs of knighthood and had been magnificently feasted, he retired to rest his weariness, while the beautiful Sabia from her balcony lulled him to sleep with her golden lute.

Úloha 6:

Zadání

OEPSAMTSDOLNRHOERSIWTGUODEAAANORRIOOSETLDNTAFEHMHKFCAWHCBAHVEGFRGH
EIRHOAREMIRNLEIUDSNTLTCOCHGTNAVTAHAEENTDGEETHNVOHTOAMPBSIUAARAGOON
DISNIHTRDHITIDHLTCOLCSSISHEAROWAIEKMODOEEIIOICEESTENVWEHMEDPSUXSEA
SLKRANDBIOWLOPSANUNOTNEHMHEHAEPSTADC

Postup

Frekvenční analýza anglický text → transpoziční šifra, obsahuje xka -> tabulka? Zkoušeno dokud x nebyly v souvislé řadě na konci sloupce 6x39, kusy textu dávaly smysl ale dohromady ne → pořadí sloupců 6. 1. 4. 3. 2. 5.

Zjištěný tip šifry

Úplná tabulka s heslem 6x39
Pořadí sloupců 6. 1. 4. 3. 2. 5.

Řešení

SO ALL SEENED HAPPINESS BUT ALAS DARK MISFORTUNE WAS AT HAND.
ALMIDOR THE BLACK KING OF MOROCCO WHO HAD LONG WOOED THE PRINCESS
SABIA IN VAIN WITHOUT HAVING THE COURAGE TO DEFEND HER SEEING THAT
THE MAIDEN HAD GIVEN HER WHOLE HEART TO HER CHAMPION RESOLVED TO
COMPASS HIS DESTRUCTION

Úloha 7:

Zadání

SEAMOEEO**T**OABISX**L**WAESM**L**WSHEMEXOTNTIOLOSTDRSXTAEUMCONIGSEAXPHUAOEFDH
NITBXGWRERBDNTIHEFXNMTBPONAFKGDOXIIEEDTALOENETYKHCHAENGTHIHCRODNTH
GANHTTRAETLATARIEGDTONHGOHAIOTOUEENACNTCHBESTOGGONAIERTAGIMHARHOEO
HEYSTRITROFDRGYPLSSHHENFOETOMSEUDCWHETTNTX

Postup

Počet jednotlivých znaků sedí s mně známým textem → transpozice. První a poslední znak sedí, tipuji tabulka. Ještě nebyla použita dvojnásobná tabulka. Zkouším všechna řešení a jedno dává smysluplný text.

Zjištěný tip šifry

dvojitá transpozice bez hesla:
první 16x15
druhá 16x15

Řešení

SOGOINGTOKINGPTOLEMYHETOLDHIMWHATWASPERCHANCETRUENAMELYTHATTHEBEAU
TEOUSSABIAHADPROMISEDSTGEORGETOBECOMECHRISTIANANDFOLLOWHIMTOENGLAN
DNOWTHETHOUGHTOFTHISSOENRAGEDTHEKINGTHATFORGETTINGHISDEBTOFHONORHE
DETERMINEDONANACTOFBASESTTREACHERYXXXXXXXX

Úloha 8:

Zadání

VCLLPDVMMVAYYMCDGBHPXRXIPXAHGXVGGXKIGJPMXTVCXHPIMGVVKMLVVYMPXYVQGI
GYYBYVLYBQDCIVVVYJGBIPABXDXIMVPJYZVMBMABMDXYGXCZZATVBVIVHGDVGCSBAK
GBIPBBDDZXDIFCJAOMGXQJYDXDPYBYIGBOAPCVIIPVTAJPDYVLVPQPBYYRYHGVPIDA
PCXGVMBDPVXKOP

Postup

Udělal jsem frekvenční analýzu na šifrovaný a výsledný text. Počty znaků odpovídali, ale byli prohozené → substituce. Prohodil jsem znaky co byli jednoznačné a zjistil že text nesedí. Zkusil jsem text hodit do tabulek různých rozměrů a při rozměru 4x53 dával částečně smysl. Doplnil jsem neznámé znaky ze substituce a prohodil sloupce aby to bylo cele správně.

Zjištěný tip šifry

kompletni substituce:

A<P;	B<K;	C<F;	D<A;	E<V;	F<Q;	G<L;
H<G;	I<B;	K<R;	L<M;	M<H;	N<C;	O<X;
P<S;	R<I;	S<D;	T<Y;	V<O;	W<J;	Y<Z

poté mřížka 4x53
pořadí řádků 4. 1. 2. 3.

Řešení

telling st george that his love and loyalty needed further trial he entrusted him with a message to the king of persia and forbade him either to také with him his horse bayard or his sword ascalon nor would he even allow him to say farewell to his beloved sabia

Úloha 9:

Zadání

RSFCQSQSLLBPMIYSYFHLIRVQRLHQJCAIXAMYCBSLOIHTSLQMGNSMMINISLSSISHMBB
CSYQQBRSIQBPHLLHVCLLCSBPARRXPERMHSNHQLLLITPSCMRPGIALOMSQQMBHYBSCHO
KLSBQGHLALCBRSTTMBLIIANISRMRMSLQXHVTLIYXMSCCMRLXRYHQTJOHSUHHSQXLTS
RQLTABLLLSIX

Postup

Zkoušel jsem rovnat text do mřížky až jsem dal 4 X za sebe. A potom jsem pomocí známého textu provedl kompletní substituci.

Zjištěný tip šifry

Úplná tabulka 14x15
Kompletní substituce

A → G	B → H	C → I	E → K	F → L	G → M	H → N
I → 0	j → P	K → Q	L → E	M → A	N → C	O → B
P → D	Q → R	R → S	S → T	T → U	U → V	V → W

Y → F

Řešení

st george then set forth sorrowfully and surmounting many dangers reached the court of the king of persia in safety but what was his anger to find that the secret missive he bore contained nothing but an earnest request to put the bearer of it to death yyyy

Literatura

Stránky předmětu
Wikipedia
http://www.tonightsbedtimestory.com/st-george-of-merrie-england-arthur-rackham/