VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

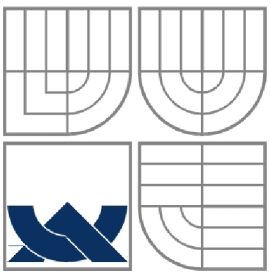
LINEÁRNA KRYPTOANALÝZA

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

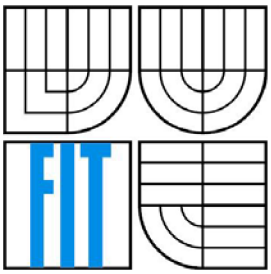
AUTOR PRÁCE
AUTHOR

JÁN KOPKO

BRNO 2007



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

LINEÁRNÍ KRYPTOANALÝZA

LINEAR CRYPTANALISYS

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE
AUTHOR

JÁN KOPKO

VEDOUCÍ PRÁCE
SUPERVISOR

doc. Ing. DANIEL CVRČEK Ph.D.

BRNO 2007

Abstrakt

Tato práce se zaobírá jedním z možných útoků na blokové šifry, lineární kryptoanalýzou. V úvodě je popsán všeobecní tvar substitučně-permutační (blokové) šifry, taktéž konkrétní šifra, na které bude lineární kryptoanalýza prezentována. Dále jsou popsané základní principy lineární kryptoanalýzy, a přehled konkrétního útoku na šifru jejím uplatněním.

Klíčová slova

kryptoanalýza, lineární kryptoanalýza, bloková šifra, permutačně-substituční šifra, útok na šifru

Abstract

This paper discusses one of possible attacks on block ciphers – linear cryptanalysis. In the beginning of this paper a basic structure of block cipher is presented, as well as concrete cipher on which the linear cryptanalysis is presented. After that basic principles of linear cryptanalysis and a preview of attack on this cipher follow.

Keywords

cryptanalysis, linear cryptanalysis, block cipher, substitution-permutation cipher, attack on cipher

Citace

Kopko Ján: Lineárna kryptoanalýza, Brno, 2007, bakalářská práce, FIT VUT v Brně.

Lineárna kryptoanalýza

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením doc. Ing. Daniela Cvrčka Ph.D.
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

……
Ján Kopko
15.5.2007

Poděkování

Ďakujem doc. Ing. Danielovi Cvrčkovi Ph.D., za odborné vedenie, rady a podnety, ktoré mi počas práce poskytoval.

Obsah

Úvod

Informácie sa čím ďalej tým viac stávajú najcennejšou komoditou moderného sveta. Ako povedal John D. Rockefeller: „*Druhou najdôležitejšou vecou po znalosti svojho obchodu je vedieť všetko o obchodoch tých ostatných.*“ Tento výrok za posledných 100 rokov prešiel z výroku slávneho bussinesmana v neotrasiteľnú pravdu o našej spoločnosti. Spoločnosti, v ktorej nevládnu v klišé často spomínané peniaze, ale čoraz viac informácie, lebo toho čo má správne informácie si peniaze nájdu.

Už v starovekom Egypte, Mezopotámii či Ríme si vládcovia uvedomovali, že informácie sú kľúčom k úspechu, a najdôležitejšie je utajiť ich pred konkurenciou. Za týmto účelom boli vyvinuté mnohé postupy, ako je šifrovanie, kódovanie alebo steganografia. Účelom všetkých troch je utajenie správy pred nechceným odhalením jej obsahu, ale tieto tri metódy sa podstatne líšia.

Pri steganogafii ide viac o skrytie správy ako o utajenie jej obsahu. Toho môžeme v dnešnej dobe docieliť napríklad použitím mikroskopického písma.

Pri kódovaní a už pracuje priamo s textom danej správy. Asi jedným z najznámejších kódov je Morseho kód, v ktorom má každé písmeno a číslo svoju akustickú či písomnú podobu. Ako istú formu kódovania by mohlo byť chápané aj obyčajné prekladanie textu z jedného jazyka do druhého. Pri tejto forme kódovania sa pracuje už nie s písmenami ale so slovami a ich ekvivalentmi v jednotlivých jazykoch. Tento spôsob utajovania správ bol použitý napríklad počas druhej svetovej vojny, keď boli pri kódovaní vojenských správ využití príslušníci amerických indiánskych kmeňov (Navaho). Vo všeobecnosti ale o kódovaní platí, že zakódovaný text si môže prečítať každý, kto má prístup k príslušnej kódovacej tabuľke (resp. slovníku.).

Poslednou metódou utajovania správ je šifrovanie. Šifrovanie na rozdiel od kódovania ale už pracuje s menšími jednotkami ako sú napríklad písmená a v dnešnej dobe bity. So šifrovaním priamo súvisia dva vedné obory, kryptografia, ktorá skúma šifrovanie správ a kryptológia, taktiež uvádzaná aj ako kryptoanalýza, ktorá sa zaoberá lúštením šifier, nachádzaním ich slabých miest a využívaním týchto k prelomeniu danej šifry.

Jednou z metód, ktoré kryptológia využíva je aj lineárna kryptoanalýza, a účelom tejto práce je predstaviť spôsob útoku touto metódou na jednoduchú blokovú šifru. Práca je rozdelená do niekoľkých kapitol, z ktorých prvá slúži ako akýsi úvod do lineárnej kryptoanalýzy. História tejto metódy je nasledovaná teoretickým princípom útoku na akúkoľvek šifru a taktiež sú tu načrtnuté potrebné prerekvizity útoku ako aj možné problémy, ktoré môžu nastať počas útoku.

Druhá kapitola predstavuje Blokové šifry, ich históriu, ktorá sa špecializuje na DES (Data Encryption Standard), ktorý inšpiroval návrhy mnohých šifier. Ďalej táto kapitola predstavuje S-box, ako asi najvýznamnejší prínos DESu pre iné šifry. V závere druhej kapitoly je predstavená konkrétna šifra, na ktorú budem v tejto práci útočiť.

Tretia kapitola už predstavuje konkrétny útok lineárnou kryptoanalýzou na mnou vybranú šifru. Táto kapitola obsahuje aproximácie šifry, ktoré sú potrebné na získanie úplného kľúča použitého pri šifrovaní, čím je šifra považovaná za zlomenú.

Záver sumarizuje výsledky dosiahnuté týmto typom útoku. Taktiež obsahuje návrhy na možné rozšírenia.

1 Lineárna kryptoanalýza

1.1 História

Lineárna kryptoanalýza bola predstavená Matsuiom v roku 1993[1]. Útok bol v dnešnej podobe prvý krát použitý na šifre DES (Data Encryption Standard), ale skoršia varianta bola úspešne použitá pri útoku na šifru FEAL (Fast Data Encryption Algorithm) v roku 1992.

Lineárna kryptoanalýza je mimo útoku hrubou silou jedným z troch útokov, ktorým sa podarilo zlomiť šifru DES. Tento typ útoku patrí do skupiny, pri ktorých musí mať útočník priamy prístup k šifre, pretože potrebuje získať čo najviac nezašifrovaných a k nim prislúchajúcich zašifrovaných textov. V pripade DESu je treba 2^{43} dvojíc. Práve kvôli tejto nevýhode je lineárna kryptoanalýza napríklad v prípade tejto šifry uvedená ako uznaná slabina šifry. Lineárna kryptoanalýza bola úspešne použita pri útoku na viacero šifier a je považovaná za veľmi silnú kryptoanalytickú metódu hlavne čo sa týka blokových šifier.

Cieľom lineárnej kryptoanalýzy pri útoku na šifru je určenie závislostí medzi paritnými bitmi zašifrovaného textu, nezašifrovaného textu a tajného kľúča. Závislosti medzi týmito paritnými bitmi sa zisťujú pomocou lineárnych aproximácií častí šifry. Útočník musí nájsť aproximáciu, ktorá by bola platná pre šifru s čo najvyššou alebo najnižšou pravdepodobnosťou. Pomocou takejto aproximácie potom môže útočník získať odhad paritného bitu kľúča, za pomoci analýzy paritných bitov zo známych zašifrovaných a nezašifrovaných textov.

1.2 Útok

1.2.1 Princíp útoku

Hlavným princípom útoku lineárnou kryptoanalýzou je vytvorenie výrazu, respektíve lineárnej aproximácie, ktorá by popisovala šifru. Pre lineárne prvky šifry, ako je napríklad šifrovanie textu kľúčom pomocou operácie XOR je ľahké nájsť výraz, ktorý by platil s pravdepodobnosťou 1. Avšak pre nelineárne prvky, ako napríklad S-box, nie je táto úloha až taká ľahká a preto treba nájsť výrazy, ktoré by mali odchýlku od 1/2 čo najväčšiu, teda aby odchýlka $\varepsilon = \left|P - 1/2\right|$ bola maximálna.

Aproximácie jednotlivých prvkov sa potom spájajú aby vytvorili aproximáciu popisujúcu jednotlivé kolá šifry a nakoniec celú šifru. Táto aproximácia by potom mala mať tvar:

$$P[i_1 \oplus i_2 \oplus \ldots \oplus i_a] \oplus C[j_1 \oplus j_2 \oplus \ldots \oplus j_b] = K[k_1 \oplus k_2 \oplus \ldots \oplus k_c] \tag{1.1}$$

respektíve:

$$P[i_1 \oplus i_2 \oplus \ldots \oplus i_a] \oplus C[j_1 \oplus j_2 \oplus \ldots \oplus j_b] \oplus K[k_1 \oplus k_2 \oplus \ldots \oplus k_c] = 0 \qquad (1.2)$$

Kde, ak budeme používať Matsuiho notáciu [1], A[*i*] reprezentuje *i*-ty bit bloku A, a A[i_1, i_2, ... i_k] reprezentuje paritný bit A[i_1] $\oplus$ A[i_2] $\oplus$ ... $\oplus$ A[i_k]. Potom P reprezentuje 16-bitový blok nezašifrovaného textu. C zastupuje blok zašifrovaného textu, a K reprezentuje bity subkľúčov použitých pri šifrovaní.

Na to aby sme paritný bit K[i_1, i_2, ... i_k] získali s čo najväčšou presnosťou potrebujeme čo najväčší počet dvojíc zašifrovaných a nezašifrovaných textov. Matsui vo svojej práci [1] odvodil vzorec, podľa ktorého je minimálny počet týchto dvojíc textov *N*, potrebný na získanie bitov subkľúča s prijateľnou presnosťou stanovený na: $N = |P - 1/2|^{-2}$, kde P je pravdepodobnosť, s ktorou výraz platí. Existujú samozrejme aj efektívnejšie algoritmy, ktoré boli vytvorené postupným zlepšovaním lineárnej kryptoanlýzy. Tieto sú popísané v [2].

1.2.2 Pilling-up lemma

Základom útoku pomocou lineárnej kryptoanalýzy je určenie aproximácie, ktorá by popisovala celú šifru s pravdepodobnosťou, ktorej absolútna odchýlka od 1/2 bola čo najvyššia. Určenie čiastočných aproximácií pre jednotlivé prvky šifry nie je veľmi zložité. Avšak pri spájaní jednotlivých čiastočných aproximácií do výrazu, ktorý by bol aplikovateľný na celú šifru vyvstáva problém, s akou pravdepodobnosťou bude platiť výsledný výraz.

Tento problém sa dá riešiť aplikáciou takzvanej „Pilling-up lemmy“. V nasledujúcej sekcii budú X_1 a X_2 reprezentovať dve náhodné binárne premenné. Základné vzťahy, ktoré platia pre tieto premenné sú:

$$X_1 \oplus X_2 = 0 \Leftrightarrow X_1 = X_2;\ X_1 \oplus X_2 = 1 \Leftrightarrow X_1 \neq X_2$$

ďalej platí že :

$$\Pr(X_1 = i) = \begin{cases} p_1 & ,i = 0 \\ 1 - p_1 & ,i = 1 \end{cases}$$

$$\Pr(X_2 = i) = \begin{cases} p_2 & ,i = 0 \\ 1 - p_2 & ,i = 1 \end{cases}$$

ak sú tieto dve premenné nezávislé tak potom:

$$\Pr(X_1 = i, X_2 = j) = \begin{cases} p_1 p_2 & ,i = 0, j = 0 \\ p_1(1 - p_2) & ,i = 0, j = 1 \\ (1 - p_1)p_2 & ,i = 1, j = 0 \\ (1 - p_1)(1 - p_2) & ,i = 1, j = 1 \end{cases}$$

na základe predchádzajúcich tvrdení môžeme ukázať, že:

$$\Pr(X_1 \oplus X_2 = 0) = \Pr(X_1 = X_2) =$$
$$= \Pr(X_1 = 0, X_2 = 0) \oplus \Pr(X_1 = 1, X_2 = 1) =$$
$$= p_1 p_2 + (1 - p_1)(1 - p_2)$$

ale keďže nás v prípade lineárnej kryptoanalýzy zaujíma hlavne odchýlka pravdepodobnosti od 1/2 môžeme nahradiť p_1 výrazom $1/2 + \varepsilon_1$ a p_2 výrazom $1/2 + \varepsilon_2$. V tom prípade by sa predchádzajúci výraz upravil do tvaru: $\Pr(X_1 \oplus X_2 = 0) = 1/2 + 2\varepsilon_1\varepsilon_2$

Výraz $X_1 \oplus X_2 = 0$ by platil s pravdepodobnosťou, ktorá by mala odchýlku od 1/2 : $\varepsilon_{1,2} = 2\varepsilon_1\varepsilon_2$

Piling-Up Lemma [1] popisuje daný princíp výpočtu pravdepodobnosti pre *n* nezávislých binárnych premenných $X_1, X_2, \ldots X_n$ tak ako je zobrazené v rovnici (1.2) nasledovne:

$$\Pr(X_1 \oplus \ldots \oplus X_n = 0) = 1/2 + 2^{n-1} \prod_{i=1}^{n} \varepsilon_i \qquad (2)$$

a odchýlka pravdepodobnosti platnosti tohto výrazu od 1/2:

$$\varepsilon = 2^{n-1} \prod_{i=1}^{n} \varepsilon_i \qquad (3)$$

Dôležitá je informácia, že ak ktorýkoľvek z výrazov X_1 až X_n platí s pravdepodobnosťou $p_i = 1/2$, potom $\Pr(X_1 \oplus \ldots \oplus X_n = 0) = 1/2$ a $\varepsilon = 0$. Takže kľúč nebude možné získať.

Aproximácia popisujúca celú šifru je vlastne reťazec aproximácií popisujúcich jednotlivé prvky šifry spojených do jedného výrazu. Takýto reťazec je nazývaný „*lineárna charakteristika*“. Za predpokladu, že jednotlivé časti lineárnej charakteristiky sú nezávislé môžeme pravdepodobnosť, s ktorou bude platiť aproximácia pre celú šifru, vypočítať podľa rovnice (2). Respektíve odchýlku tejto pravdepodobnosti od 1/2 vypočítať pomocou rovnice (3).

Základným problémom Pilling-up lemmy je predpoklad, že všetky výrazy použité vo výslednej aproximácii sú navzájom nezávislé. Tento predpoklad je často nesplniteľný, keďže výstup jedného z prvkov šifry je zároveň vstupom druhého. Taktiež subkľúče použité v jednotlivých kolách šifry nemusia spĺňať tento predpoklad, keďže sú vo väčšine prípadov získavané z jedného hlavného kľúča. Práve preto je dôležité uviesť, že aj keď sú predpoklady získané na základe Pilling-up lemmy vo veľkom prípade praktických využití veľmi presné, môže nastať situácia keď bude skutočná odchýlka rozdielna od tej teoretickej.

1.2.3 Linear hull

V predchádzajúcej sekcii je popísaný postup ako sa dá vypočítať odchýlka aproximácie popisujúcej celú šifru vytvorením takzvanej lineárnej charakteristiky. V niektorých prípadoch sa daná odchýlka výrazne líši od tej, ktorú získame útokom na šifru. Dôvodom pre tento rozdiel nemusí byť len chybný

predpoklad o nezávislosti jednotlivých výrazov pri aplikácii Pilling-up lemmy. Ďalším z dôvodov výrazného rozdielu medzi teoretickou a skutočnou odchýlkou pravdepodobnosti platnosti danej aproximácie môže byť aj takzvaný „*linear hull efekt*“.

Pojem „*linear hull efekt*“ bol zavedený K. Nybergovou v roku 1994 [3]. Tento efekt nastane ak sa daná aproximácia celej šifry dá popísať viacerými lineárnymi charakteristikami. Lineárne charakteristiky, ktoré majú rovnaký vstup a výstup, ale obsahujú inú množinu bitov kľúča (to znamená, že využívajú iné prvky šifry), spolu tvoria takzvaný „*linear hull*“.

Potom na základe hodnôt bitov kľúča sa jednotlivé lineáne charakteristiky ovplyvňujú. Ak sú množiny bitov kľúčov použitých v rôznych charakteristikách nezávislé, potom môže dôjsť k zníženiu absolútnej odchýlky a tým zníženiu pravdepodobnosti úspechu útoku na šifru. Avšak algoritmy popísané v [2] sú navrhnuté tak aby linear hull efekt využili vo svoj prospech.

1.2.4 Odolnosť voči lineárnej kryptoanalýze

Ak hlavnou úlohou pri útoku lineárnou kryptoanalýzou je nájdenie lineárnej aproximácie, ktorá by popisovala šifru, potom jednoznačným dôkazom odolnosti šifry voči lineárnej kryptoanalýze by bol dôkaz, že takáto aproximácia neexistuje. Tento dôkaz je však veľmi náročný aj pre jednoduché šifry, a nie je úplne potrebný, pretože stačí dokázať, že šifra je napadnuteľná lineárnou kryptoanalýzou, ale tento útok by bol minimálne tak náročný ako útok hrubou silou.

To znamená, že najlepšia aproximácia šifry bude mať odchýlku, takú že počet potrebných dvojíc nezašifrovaných a zašifrovaných textov na útok bude minimálne 2^n, kde *n* udáva šírku šifry. Počet potrebných dvojíc textov N na útok lineárnou kryptoanalýzou Matsui stanovil na $N = \varepsilon^{-2}$. To znamená, že pre $\varepsilon \leq 1/\sqrt{2^n}$, kde *n* reprezentuje šírku šifry, treba na útok lineárnou kryptoanalýzou všetky dvojice zašifrovaných a nezašifrovaných textov (pri rovnosti), respektíve útok nie je uskutočniteľný (ak je ε menšie). Avšak takýto predpoklad je treba prakticky overiť, keďže netreba zabúdať na linear hull efekt a taktiež na vplyv pilling-up lemmy ak bola táto použitá pri výpočte odchýlky danej aproximácie.

2 Blokové šifry

2.1 Prehľad

Blokové šifry patria medzi symetrické šifry, ktoré šifrujú skupiny bitov rovnakej dĺžky, bloky, stále rovnaký postupom. Pri šifrovaní má bloková šifra na vstupe blok bitov (napríklad 64, 128 alebo 256), a na výstupe rovnako veľký blok zašifrovaného textu. Na šifrovaní základného textu sa podieľa aj druhý vstup, ktorým je tajný kľúč. Tento kľúč je zdieľaným tajomstvom medzi oboma stranami, ktoré si vymieňajú danú informáciu. Takže v skutočnosti má bloková šifra na vstupe nezašifrovanú správu a tajný kľúč a na výstupe zašifrovaný text. Dešifrovanie je potom inverzný algoritmus, ktorý má na vstupe zašifrovaný text a rovnaký tajný kľúč a jeho výstupom je pôvodná správa.

Môžeme teda napísať, že bloková šifra sa skladá z dvoch algoritmov, jeden na šifrovanie a druhý na dešifrovanie, o ktorých platí, že sú navzájom inverzné. Teda ak označíme šifrovací algoritmus E a dešifrovací algoritmus D, potom $E_K(D_K(B)) = B$, pre každý blok B a kľúč K.

Za prvú blokovú šifru je považovaná šifra Lucifer vytvorená spoločnosťou IBM v roku 1970. V roku 1976 bola verejnosti predstavená asi najznámejšia bloková šifra - DES (Data Encryption Standard). Aj napriek pôvodným obavám bol DES prijatý ako štandard v novembri 1976 ako štandard FIPS PUB 46 [4]. Posledná aktualizácia DESu bola v roku 2001 [5].

DES sa skoro po svojom uvedení presadil a celosvetovo sa rozšíril. Od jeho zavedenia bol ako základ blokových šifier považovaný 64-bitový blok dát. DES taktiež predstavil „S-boxy“ (substitution boxy). Pôvodne bolo na tieto prvky nazerané s nedôverou, pretože na ich návrhu sa podieľala NSA (National Security Agency – Národná bezpečnostná agentúra USA) a preto panovalo podozrenie, že majú nejakú slabosť, ktorú je NSA schopná využiť a dostať sa tak k citlivým informáciám. Tieto pochybnosti boli rozptýlené v roku 1990 pri verejnej prezentácii diferenciálnej kryptoanalýzy [6, 7].

V roku 1994 bola na DESe prezentovaná po prvýkrát lineárna kryptoanalýza [1]. Aj keď na zlomenie DESu potrebuje oproti diferenciálnej kryptoanalýze menej známych dvojíc nezašifrovaných a zašifrovaných blokov (2^{43} oproti 2^{47}) je tento útok nepraktický, ale ako kryptoanalytický nástroj je používaná na zlepšenie odolnosti nových šifier. A pri návrhoch nových šifier je dnes vyžadované aby boli tieto odolné ako proti útoku lineárnou tak aj diferenciálnou kryptoanalýzou.

DES bol prvý krát prelomený útokom hrubou silou v roku 1997. Tento útok spočíva v aplikovaní všetkých možných kľúčov na zašifrovaný text za účelom získania pôvodnej nezašifrovanej správy. DES bol zlomený DESCHAL projektom za 96 dní. Už 2. januára 1997 bola ohlásená verejná súťaž za účelom nájdenia nástupcu DESu. Za úplný koniec DESu by mohol byť

považovaný január 1999, v ktorom sa za spoločného úsilia Deep Crack-u a disturbed.net podarilo zlomiť DES útokom hrubou silou za 22 hodín a 15 minút [8].

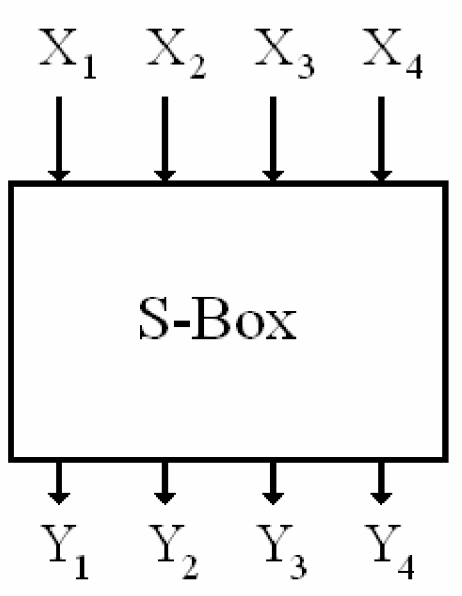
Odpoveďou na tento útok bolo zavedenie takzvaného „Triple DES“ (TDES) [5], ktorý využíva dva alebo tri kľúče a je založený na trojnásobnom postupnom použití DESu. V novembri 2001 bol ako nástupca DESu predstavený AES (Advanced Encryption Standard), ktorým sa stala šifra Rijndael od autorov V. Rijmena a J.Daemena, ktorá bola vybraná z pätnástich kandidátov na základe verejnej súťaže. AES bol v roku 2001 prijatý ako štandard NIST FIPS PUB 197 [10]. DES bol oficiálne stiahnutý ako štandard v máji roku 2005.

2.2 DESu podobné šifry

2.2.1 S-box

S-box (subsitution box) je významným prínosom DESu. Tento prvok šifry by mohol byť chápaný ako skrinka (box) so štyrmi vstupnými a štyrmi výstupnými bitmi (Obrázok 1). Základným princípom fungovania S-boxu je, aby substitúcia vstupných bitov na výstupné nebola lineárna, to znamená aby nebolo možné ju popísať lineárnou funkciou.

Obrázok 1:



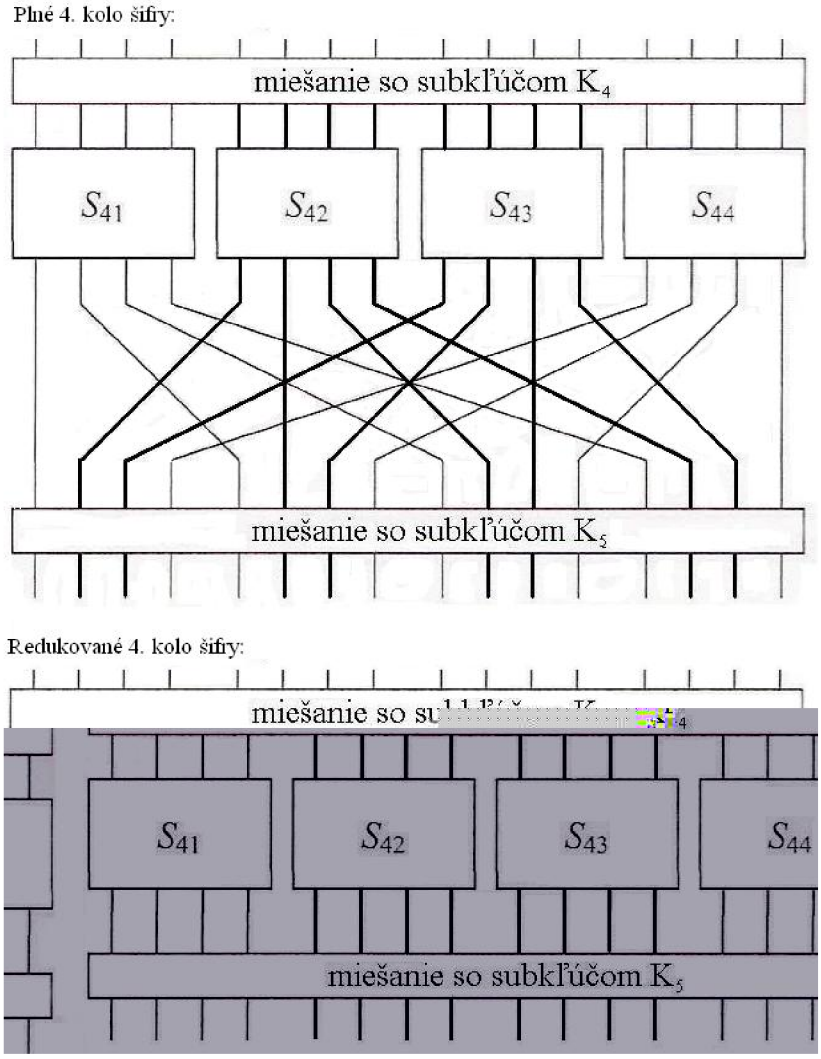
DES predstavil množinu 32 S-boxov. Šifry inšpirované DESom vo väčšine prípadoch používajú niektoré (alebo všetky) S-boxy z tejto množiny, keďže pri vytváraní vlastného S-boxu sa nemusí dodržať nelinearita tohto prvku, čo môže viesť k vytvoreniu slabého miesta v šifre, ktoré by bolo náchylné na útok tohto typu. Čo značí že by mohol byť takto vytvorený S-box reprezentovaný výrazom, ktorý by bol pravdivý s pravdepodobnosťou 1 alebo 0.

2.2.2 Substitučno-permutačná šifra

Na predstavenie lineárnej kryptoanalýzy som si vybral jednoduchú substitučno-permutačnú šifru, ktorá pracuje nad 16-bitovým blokom dát. Šifra pracuje s tromi základnými prvkami, ktoré periodicky opakuje. Týmito prvkami sú substitúcia, ktorá je realizovaná pomocou S-boxov, ďalej permutácia a napokon zanášanie kľúča, ktoré je realizované jednoduchou funkciou XOR. Táto základná štruktúra bola predstavená v roku 1973 H. Feistelom [11], a podobnú štruktúru má napríklad aj DES a AES.

Prehľadný nákres celej šifry je v prílohe 1. Šifra sa skladá z štyroch kôl, čo znamená, že sa všetky operácie zopakujú štyri krát a potom sa uskutoční ešte záverečné zanášanie kľúča, aby nebolo možné posledné kolo spätne dešifrovať. Avšak skutočná realizácia, ktorú som sa rozhodol použiť v poslednom kole neobsahuje permutáciu, takže má posledné kolo redukované. Pre túto zmenu som sa rozhodol z čisto zištných dôvodov, a teda aby bity posledného kľúča, ktoré sa budem snažiť získať tvorili súvislí blok, tak ako je to ukázané na obrázku číslo 2. Táto redukcia nijak neovplyvňuje odolnosť šifry voči útoku lineárnou kryptoanalýzou.

Obrázok 2:



Všetky S-boxy zobrazené v prílohe 1. sú rovnaké. A pre potreby tejto práce som sa rozhodol použiť S-box prezentovaný šifrou DES, konkrétne sa jedná o prvý riadok z prvej skupiny použitej pri šifrovaní DESu [12]. Asi najjednoduchším spôsobom reprezentácie S-boxu je vyhľadávacia tabuľka, v ktorej je každému možnému vstupu S-boxu priradený odpovedajúci výstup.

Tabuľka 1: Reprezentácia S-boxu vyhľadávacou tabuľkou

VSTUPNÉ BITY	VÝSTUPNÉ BITY
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

3 Útok

3.1 Popis S-boxu

Keďže S-box nie je lineárnym prvkom jedinou možnosťou ako popísať jeho správanie je vytvoriť výraz, ktorý by ho aspoň približne charakterizoval. Keďže celá lineárna kryptoanalýza sa snaží nájsť závislostí medzi paritnými bitmi bude mať aj aproximácia S-boxu tvar výrazu (1.1) (kapitola 1.2.1).

S-box má na vstupe aj výstupe 4 bity, takže týchto výrazov bude existovať $2^4 * 2^4 = 256$. Aby sme mohli vybrať z tejto množiny ten, ktorý najlepšie poslúži nášmu útoku musíme zistiť s akou pravdepodobnosťou sú jednotlivé výrazy pravdivé. Táto úloha je realizovateľná pomocou pravdivostnej tabuľky. Takáto tabuľka by napríklad pre výraz $X_1 \oplus X_2 \oplus X_3 \oplus X_4 = Y_2 \oplus Y_3 \oplus Y_4$ vyzerala nasledovne:

Tabuľka 2:

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	L: $X_1 \oplus X_2 \oplus X_3 \oplus X_4$	R: $Y_2 \oplus Y_3 \oplus Y_4$	L = R
0	0	0	0	1	1	1	0	0	0	x
0	0	0	1	0	1	0	0	1	1	x
0	0	1	0	1	1	0	1	1	0	
0	0	1	1	0	0	0	1	0	1	
0	1	0	0	0	0	1	0	1	1	x
0	1	0	1	1	1	1	1	0	1	
0	1	1	0	1	0	1	1	0	0	x
0	1	1	1	1	0	0	0	1	0	
1	0	0	0	0	0	1	1	1	0	
1	0	0	1	1	0	1	0	0	1	
1	0	1	0	0	1	1	0	0	0	x
1	0	1	1	1	1	0	0	1	1	x
1	1	0	0	0	1	0	1	0	0	x
1	1	0	1	1	0	0	1	1	1	x
1	1	1	0	0	0	0	0	1	0	
1	1	1	1	0	1	1	1	0	1	

Z tabuľky vyplýva, že výraz $X_1 \oplus X_2 \oplus X_3 \oplus X_4 = Y_2 \oplus Y_3 \oplus Y_4$ je pravdivý s pravdepodobnosťou 1/2. To znamená, že je ako aproximácia môjho S-boxu je nepoužiteľný. Toto je však príklad iba jedného výrazu. Tabuľka 3 obsahuje všetky možné výrazy, ktoré by mohli poslúžiť ako aproximácie jednotlivých S-boxov v mojej šifre.

Vstupné aj výstupné bity S-boxu sú v nej reprezentované hexadecimálnym číslom. Predchádzajúci výraz môžeme nájsť v riadku označenom číslom 7 a v stĺpci označenom F. Čísla v tabuľke označujú počet prípadov, v ktorých je výraz pravdivý (ľavá strana výrazu sa rovná pravej).

Tabuľka 3

		Vstupné bity S-boxu														
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Výstupné bity	**1**	8	8	8	10	6	10	6	8	8	12	12	6	10	10	6
	2	6	6	8	8	6	6	8	8	6	6	8	12	10	10	4
	3	6	6	8	6	8	12	10	8	6	10	4	6	8	8	6
	4	8	8	8	6	6	10	10	8	8	4	12	6	6	6	6
	5	8	8	8	4	8	8	4	8	8	8	8	8	12	4	8
	6	6	6	8	6	12	8	10	8	6	10	12	10	8	8	10
	7	14	6	8	8	10	10	8	8	6	6	8	8	10	10	8
	8	10	8	10	8	6	8	6	6	4	10	8	10	4	6	8
	9	10	8	2	6	8	6	8	10	8	10	8	8	6	8	6
	A	8	10	6	8	4	10	10	10	6	8	8	10	10	8	12
	B	8	10	6	10	10	12	8	6	10	8	8	12	8	6	6
	C	10	8	10	10	8	6	12	10	8	10	8	8	10	4	6
	D	10	8	10	4	6	8	10	6	12	10	8	10	8	10	8
	E	8	2	6	10	6	8	8	6	10	8	8	8	8	6	10
	F	8	10	6	8	8	6	10	2	6	8	8	6	10	8	8

Na základe tejto tabuľky máme dostupné informácie o všetkých možných aproximáciách S-boxov v šifre. Potom vhodným spájaním S-boxov a využitím vhodných aproximácií som bol schopný vytvoriť dve aproximácie, pomocou ktorých sa dá uskutočniť útok lineárnou kryptoanalýzou a tým získať hodnotu subkľúča použitého po štvrtom kole šifry. Tieto aproximácie som si nazval X a Y a ich podrobná štruktúra je zachytená v nasledujúcich kapitolách. Obe aproximácie nepopisujú celú šifru, ale len jej tri kolá. To preto, aby bola aproximácia použiteľná pri útoku na šifru.

3.2 Aproximácia X

Táto aproximácia využíva S-boxy S_{12}, S_{22}, S_{24}, S_{32}, S_{34}, tak ako je to zobrazené v Prílohe 2. Pre tieto S-boxy použijeme nasledujúce aproximácie:

$S_{12} : X_1 \oplus X_2 \oplus X_4 = Y_2 \oplus Y_4$ platí s pravdepodobnosťou 3/4

$S_{22}, S_{24} : X_2 = Y_2 \oplus Y_4$ platí s pravdepodobnosťou 1/4

$S_{32}, S_{34} : X_3 \oplus X_4 = Y_1 \oplus Y_3$ platí s pravdepodobnosťou 1/4

V nasledujúcej sekcii budeme používať Matsuiho notáciu [1]. I_i bude reprezentovať 16-bitový blok bitov na vstupe S-boxov v i-tom kole. $I_i[j]$ reprezentuje j-ty bit bloku I_i a nakoniec $I_i[a, b, c \ldots]$ reprezentuje paritný bit $I_i[a] \oplus I_i[b] \oplus I_i[c] \oplus \ldots$. Potom O_i reprezentuje 16-bitový blok bitov na výstupe S-boxov v i-tom kole. Bity v bloku sú číslované od 1 do 16 zľava doprava viď. Príloha 1. Podobne K_i reprezentuje 16-bitový blok bitov subkľúča v i-tom kole šifry. Výnimkou je K_5, ktorý reprezentuje blok využitý po štvrtom kole šifry. P reprezentuje blok nezašifrovaného textu.

Na základe tejto anotácie môžeme napísať, že $I_1 = K_1 \oplus P$. Takže aproximácia S-boxu S_{14} bude podľa danej anotácie vyzerať nasledovne:

$$S_{12} : I_1[5,6,8] = O_1[6,8]$$

Aproximácia tohto S-boxu je zároveň aproximáciou celého prvého kola šifry. A tento výraz sa ďalej upraviť, tak aby zahŕňal bity nezašifrovaného textu:

$$X_1 : P[5,6,8] \oplus K_1[5,6,8] \oplus O_1[6,8] = 0 \quad (4)$$

Táto aproximácia je pravdivá s pravdepodobnosťou $PX_1 = 3/4$.

V druhom kole sú aktívne (využité) už dva S-boxy, a to S_{22} a S_{24}. Takže aproximáciu druhého kola získame využitím pilling-up lemmy na tieto S-boxy:

$$S_{22} : I_2[6] = O_2[6,8]$$
$$S_{24} : I_2[14] = O_2[14,16]$$

Keďže platí, že $I_2[6] = O_1[6] \oplus K_2[6]; I_2[14] = O_1[8] \oplus K_2[14]$. Potom aproximácia druhého kola šifry bude vyzerať:

$$X_2 : O_1[6,8] \oplus K_2[6,14] \oplus O_2[6,8,14,16] = 0 \quad (5)$$

Tento výraz bude platný s pravdepodobnosťou $PX_2 = 1/2 + 2*(1/4 - 1/2)^2 = 5/8$

Tretie kolo podobne ako to druhé má dva aktívne S-boxy:

$$S_{32} : I_3[6,8] = O_3[5,7]$$
$$S_{34} : I_3[14,16] = O_3[13,15]$$

Výsledná aproximácia tretieho kola aj s úpravou aby zahŕňala výstupné bity S-boxu S_{24} vyzerá nasledovne:

$$X_3 : O_2[6,8,14,16] \oplus K_3[6,8,14,16] \oplus O_3[5,7,13,15] = 0 \quad (6)$$

Keďže aproximácie S-boxov použitých v treťom kola platia s rovnakou pravdepodobnosťou ako aproximácie S-boxov z druhého kola, bude to platiť aj o výslednej aproximácii:

$$PX_3 = 1/2 + 2*(1/4 - 1/2)^2 = 5/8$$

Podobným spôsobom získame spojením aproximácií prvých troch kôl šifry výraz, ktorý ich popisuje ako celok. Spojením výrazov (4),(5) a (6) samozrejme dôjde k eliminovaniu niektorých prvkov, keďže platí že $Z \oplus Z = 0$. Výsledkom tohto spojenia je výraz:

$$X : P[5,6,8] \oplus K_1[5,6,8] \oplus K_2[6,14] \oplus K_3[6,8,14,16] \oplus O_3[4,7,13,15] = 0$$

Tento výraz sa dá ešte upraviť tak, aby obsahoval vstupné bity S-boxov štvrtého kola. Takto upravený výraz bude vyzerať:

$$X : P[5,6,8] \oplus K_1[5,6,8] \oplus K_2[6,14] \oplus K_3[6,8,14,16] \oplus K_4[2,4,10,12] \oplus I_4[2,4,10,12] = 0 \quad (7)$$

Tento výraz bude platiť s pravdepodobnosťou:

$$PX = 1/2 + 2^2 * (PX_1 - 1/2) * (PX_2 - 1/2) * (PX_3 - 1/2) =$$
$$= 1/2 + 2^2 * (3/4 - 1/2) * (5/8 - 1/2) * (5/8 - 1/2) = 33/64$$

Odchýlka tohto výrazu sa rovná $\varepsilon_X = 33/64 - 1/2 = 1/64$. To znamená, že minimálny počet známych dvojíc zašifrovaných a nezašifrovaných textov je $N_X = \varepsilon_X^{-2} = (64)^2 = 4096$.

3.3 Aproximácia Y

Táto aproximácia využíva S-boxy S_{12}, S_{22}, S_{32}, S_{34}, a je zobrazená v prílohe 3. Aproximácie jednotlivý použitých S-boxov sú nasledovné.

$S_{12} : X_1 \oplus X_3 \oplus X_4 = Y_2$ platí s pravdepodobnosťou 1/4

$S_{22}, S_{32}, S_{34} : X_2 = Y_2 \oplus Y_4$ platí s pravdepodobnosťou 1/4

Označenia jednotlivých bitov, respektíve blokov bitov sú rovnaké ako v predchádzajúcej sekcii. Pri tejto druhej fáze sa v prvom aj druhom kole nachádza iba jeden S-box. Takže aproximácie týchto kôl budú dosť jednoduché, a vyzerajú nasledovne. Prvé kolo šifry:

$$Y_1 : P[5,7,8] \oplus K_1[5,7,8] \oplus O_1[6] = 0 \quad (8)$$

Tento výrok platí s pravdepodobnosťou : $PY_1 = 1/4$

Druhé kolo:

$$Y_2 : O_1[6] \oplus K_2[6] \oplus O_2[6,8] = 0 \tag{9}$$

Tento výrok bude taktiež pravdivý s pravdepodobnosťou $PY_2 = 1/4$

V treťom kole sú už aktívne dva S-boxy:

$$Y_3 : O_2[6,8] \oplus K_3[6,14] \oplus O_3[6,8,14,16] = 0 \tag{10}$$

Tento výrok bude taktiež pravdivý s pravdepodobnosťou $PY_3 = 1/2 + 2*(1/4 - 1/2)^2 = 5/8$

Spojením výrazov (8),(9) a (10) vznikne aproximácia, ktorá bude popisovať znova prvé tri kolá šifry, a to nasledujúcim spôsobom:

$$Y : P[5,7,8] \oplus K_1[5,7,8] \oplus K_2[6] \oplus K_3[6,14] \oplus K_4[6,8,14,16] \oplus I_4[6,8,14,16] = 0 \tag{11}$$

Pravdepodobnosť, s akou bude táto aproximácia pravdivá sa znova dá zistiť aplikáciou pilling-up lemmy, takže:

$$PY = 1/2 + 2^3 * (PY_1 - 1/2) * (PY_2 - 1/2) * (PY_3 - 1/2) =$$
$$= 1/2 + 2^3 * (1/4 - 1/2)^2 * (5/8 - 1/2) = 17/32$$

Odchýlka tohto výrazu sa rovná $\varepsilon_y = 17/32 - 1/2 = 1/32$. To znamená, že minimálny počet známych dvojíc zašifrovaných a nezašifrovaných textov je $N_y = \varepsilon_y^{-2} = (32)^2 = 1024$.

3.4 Získanie kľúča

Keď raz máme lineárnu aproximáciu popisujúcu N-1 kôl N kolovej šifry, môžeme pristúpiť k útoku na šifru a tak získať bity posledného subkľúča. V našom prípade sa jedná o subkľúč K_5. Tento proces zahŕňa čiastočné dešifrovanie posledného kola šifry. Toto dešifrovanie musí byť prevedené pre všetky možnosti ktoré môže subkľúč nadobúdať. Zároveň pre každú kombináciu subkľúča využijeme všetky dostupné zašifrované a nezašifrované texty, ktoré máme k dispozícii pre danú šifru. Tento proces vykonáme pre obe aproximácie z predchádzajúcich sekcií a tým získame plných 16 bitov posledného subkľúča. Z toho vyplýva, že pri útoku budeme v oboch prípadoch riešiť po 256 možností, ktoré môžu jednotlivé časti subkľúča nadobudnúť. Potom musíme zistiť v koľkých prípadoch sú obe výsledné aproximácie X a Y pravdivé.

Bity z bloku I_4 dostaneme dekryptovaním posledného kola šifry pomocou daného subkľúča, ktorý práve skúmame. Pre každú kombináciu subkľúča a dvojice známych textov potom zistime či je aproximácia pravdivá. Tu sa objavuje problém s bitmi ostatných subkľúčov, o ktorých nemáme žiadne informácie. Riešenie tohto problému nie je nijak zložité. V oboch prípadoch môžeme bity ostatných subkľúčov „skryť“ do pomocnej premennej a to nasledovne:

$$X : P[5,6,8] \oplus \Sigma_{KX} \oplus I_4[2,4,10,12] = 0;$$
$$\Sigma_{KX} = K_1[5,6,8] \oplus K_2[6,14] \oplus K_3[6,8,14,16] \oplus K_4[2,4,10,12]$$
$$Y : P[5,7,8] \oplus \Sigma_{KX} \oplus I_4[6,8,14,16] = 0;$$
$$\Sigma_{KX} = K_1[5,7,8] \oplus K_2[6] \oplus K_3[6,14] \oplus K_4[6,8,14,16]$$

V oboch prípadoch môže Σ_{KX} nadobúdať iba hodnoty 1, alebo 0. Preto môžeme prehlásiť, že ak výraz X platí s pravdepodobnosťou 33/64 pre Σ_{KX} rovné 0, potom ak Σ_{KX} bude rovné 1 bude výraz X platiť s pravdepodobnosťou 1-33/64 = 31/64. Dôležitá je však skutočnosť, že absolútna hodnota zostáva stále rovnaká a to v tomto prípade 1/32. Tento fakt znamená, že pravdepodobnosť úspechu útoku sa vynechaním hodnôt bitov ostatných subkľúčov nijak nezníži.

To znamená, že bity bloku P máme priamo k dispozícii prostredníctvom nezašifrovaných textov, ktoré sú k útoku nevyhnutné. Bity z blokov K_1 až K_4 vynecháme a bity bloku I_4 získame spätným postupom šifrou tak, že si za potrebné bity bloku K_5 dosadíme všetky možné kombinácie (je ich 512, keďže útok má dve časti) postupne pre všetky možné zašifrované texty. Ak sa potom aproximácia X, alebo Y ukáže pravdivá pre konkrétnu kombináciu ukáže pravdivá inkrementujeme dané počítadlo subkľúča. Týchto počítadiel musíme mať 1024, keďže je 256 kombinácii subkľúčov v dvoch útokoch a sú dve aproximácie.

Na útok bolo použitých 5000 dvojíc nezašifrovaných a zašifrovaných textov. Nasledujúce tabuľky ukazujú tie kombinácie kľúčov, ktorých odchýlka od 2500 bola čo najvyššia.

Tabuľka 4.: Čiastočné výsledky útoku aproximáciou X:

čiastočný subkľúč : bity 1-4 a 9-12		počet platných aproximácií	odchýlka od 2500
6	3	2308	192
6	15	2647	147
7	3	2360	140
6	14	2638	138
6	13	2377	123
5	3	2613	113
0	3	2389	111
6	2	2390	110
11	3	2607	107
4	3	2606	106
7	13	2397	103
7	15	2603	103
10	3	2600	100
4	5	2401	99
1	3	2402	98
0	14	2595	95
6	1	2595	95
4	15	2411	89
2	0	2414	86
6	0	2586	86
7	14	2586	86
2	2	2584	84

Tabuľka 5.: Čiastočné výsledky útoku aproximáciou Y:

čiastočný subkľúč : bity 5-8 a 13-16		počet platných aproximácií	odchýlka od 2500
1	1	2628	128
3	4	2624	124
13	4	2595	95
10	5	2589	89
3	7	2412	88
3	10	2588	88
1	3	2415	85
15	14	2415	85
3	9	2418	82
12	1	2418	82
0	11	2419	81
13	14	2579	79
6	7	2576	76
14	7	2576	76
0	9	2575	75
0	1	2573	73
2	13	2572	72
6	5	2428	72
14	10	2428	72
15	4	2429	71
6	12	2569	69
13	1	2431	69
13	6	2431	69

Z týchto tabuliek sa dá vyvodiť niekoľko predpokladov. Napríklad z prvých riadkov tabuľky 4 je možné usúdiť, že subkľúč bude vyzerať : $K_5 = [0110xxxx0011xxxx]$. To sa dá usúdiť, nielen podľa najvyššej odchýlky, ktorú dosiahla kombinácia [6,3] v tomto útoku, ale aj podľa ďalších riadkov tejto tabuľky, v ktorých majú rôzne kombinácie na mieste bitov 1 až 4 najčastejšie číslo 6 a na mieste bitov 9 až 12 číslo 3.

Oproti tomu nemá tabuľka nemá vôbec jednoznačné výsledky, keďže rozdiel 2 pri 5000 pokusoch je doslova zanedbateľný. Vplyv na tento výsledok ako je uvedené v kapitolách 1.2.2 a 1.2.3 môže mať linear hull efekt, ako aj samotná aplikácia pillinh-up lemmy pri zisťovaní pravdepodobnosti s ktorou bude výsledná aproximácia pravdivá.

Ďalším zaujímavým úkazom je reálna odchýlka pri týchto útokoch. V aproximácii bola predpokladaná odchýlka stanovená na 1/64, čo je 0,015625, kým kombinácia [6,3] pri tomto útoku dosiahla hodnoty 0,0384, čo je dvojnásobne viac ako sa dalo predpokladať. Na druhej strane matematicky určená približná hodnota odchýlky v prípade aproximácie Y bola stanovená na 1/32. Pri praktickom útoku dosiahla najlepšia odchýlka len niečo viac ako 80% tejto hodnoty. Znovu treba pripomenúť, že vplyv na tento úkaz mohol mať linear hull efekt, alebo predpoklad, že výrazy použité pri aplikácii sú lineárne nezávislé. Vplyv na tento úkaz však mohli mať aj použité dvojice

nezašifrovaných a zašifrovaných textov. Pri použití iných 5000 prvkov môžu výsledky byť odlišné. Odlišnosť však môže nastať len do istej miery.

Faktom ostáva, že šifru sa podarilo zlomiť. Určenie ktorý z dvoch možných kandidátov:

$$1.: K_{5A} = [0110.0001.0011.0001]$$
$$2.: K_{5B} = [0110.0011.0011.0100]$$

je tým správnym by pravdepodobne vyriešilo vytvorenie ešte jednej aproximácie, ktorá by prechádzala inými prvkami šifry. Druhým spôsobom ako zistiť, ktorý z dvoch kandidátov je ten správny by bolo rozšírenie počtu dvojíc nezašifrovaných a zašifrovaných textov pri útoku,.

4 Záver

V tejto práci bola predstavená lineárna kryptoanalýza, ako jeden z možných útokov na symetrické blokové šifry. V práci je načrtnutý obrys útoku na akúkoľvek šifru pomocou lineárnej kryptoanalýzy, ktorý je nasledovaný praktickým príkladom útoku na jednoduchú substitučno-permutačnú šifru. Útok je štruktúrovaný tak, aby poskytol kompletný prehľad o tejto kryptoanalytickej metóde, od jej matematických predpokladov, cez analýzu jednotlivých prvkov šifry, až k samotnému vytvoreniu lineárnej aproximácie, ktorá je použitá na získanie tajného kľúča, ktorý bol použitý pri šifrovaní.

Aj keď výsledkom celého útoku nebol jeden jednoznačný kandidát, skutočnosť, že sa podarilo eliminovať počet možných použitých kľúčov z vyše 65000 na dva by mohla byť považovaná za úspech práce ako celku.

Možné rozšírenie práce by som videl v aplikácii získaných poznatkov o lineárnej kryptoanlýze na útok na niektorú z dnes používaných blokových šifier. Inou variantov by mohol byť útok na rovnakú šifru pomocou inej metódy, ako napríklad diferenciálnej kryptoanalýzy a iných, a porovnanie výsledkov jednotlivých útokov, ich časovú náročnosť nie len algorimtu, ale aj náročnosť hľadania správnej cesty útoku kryptoanalytikom. Podobné porovnanie, by ale s najväčším predpokladom vyžadovalo výber novej a zložitejšej šifry, pretože výsledky na jednoduchej šifre tohto typu by mohli byť skresľujúce.

Literatúra

[1] M. Matsui. "*Linear Cryptanalysis Method for DES Cipher*", Advances in Cryptology, EUROCRYPT '93 (Lecture Notes in Computer Science no. 765), Springer-Verlag, pp. 386-397, 1994.

[2] L. R. Knudsen and M. J. B. Robshaw. "*Non-linear aproximations in linear cryptanalisys*", Proceedings of EUROCRYPT '96 (Lecture Notes in Computer Science no. 1070), Springer-Verlag, pp. 224-236, 1996.

[3] K. Nyberg. "*Linear aproximations of block ciphers*", Advances in Cryptology, EUROCRYPT '94 (Lecture Notes in Computer Science no. 950), Springer-Verlag, pp. 439-444, 1995.

[4] National Bureau of Standards. "*Data Encryption Standard*", Federal Information Processing Standard 46, 1977.

[5] National Bureau of Standards. "*Data Encryption Standard*", Federal Information Processing Standard 46-3, 1999.
[13.5.2007] URL: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[6] E. Biham, A.Shamir. „*Diferential cryptanalysis of DES-like cryptosystems*“, Advances in Cryptology – CRYPTO 1990. Springer-Verlag, pp. 2-21, 1990

[7] E. Biham, A.Shamir. „*Diferential cryptanalysis of DES*“, Springer-Verlag, 1993, ISBN 0-387-97930-1, ISBN 3-540-97930-

[8] DES challenges. 2007, [13.5.2007] URL: http://en.wikipedia.org/wiki/DES_Challenges

[9] National Bureau of Standards. "*Advanced Encryption Standard*", Federal Information Processing Standard 197, 2001.
[13.5.2007] URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[10] National Institute of Standards and Technolgy – Federal Iformation Procesing Standards. 2007, [13.5.2007] URL: http://csrc.nist.gov/publications/fips/

[11] H. Feistel. "*Cryptography and Computer Privacy*", *Scientific American*, vol. 228, no. 5, 1973.

[12] DES Encryption. 2007, [13.5.2007] URL: http://www.tropsoft.com/strongenc/des.htm

[13] E. Biham. „*On Matsui's linear cryptanalisys*“, Springer-Verlag, 1998

[14] A. J. Menezes, P. C. van Oorschot, S. A. Vanstome. "*Handbook of applied cryptography*", CRC Press, 1996, 816 pages, ISBN: 0-8493-8523-7

[15] H. M. Heys. "*A Tutorial on Linear and Differential Cryptanalysis*", Technical Report CORR 2001-17, Centre for Applied Cryptographic Research, Department of Combinatorics and Optimization, University of Waterloo, Mar. 2001.

Zoznam príloh

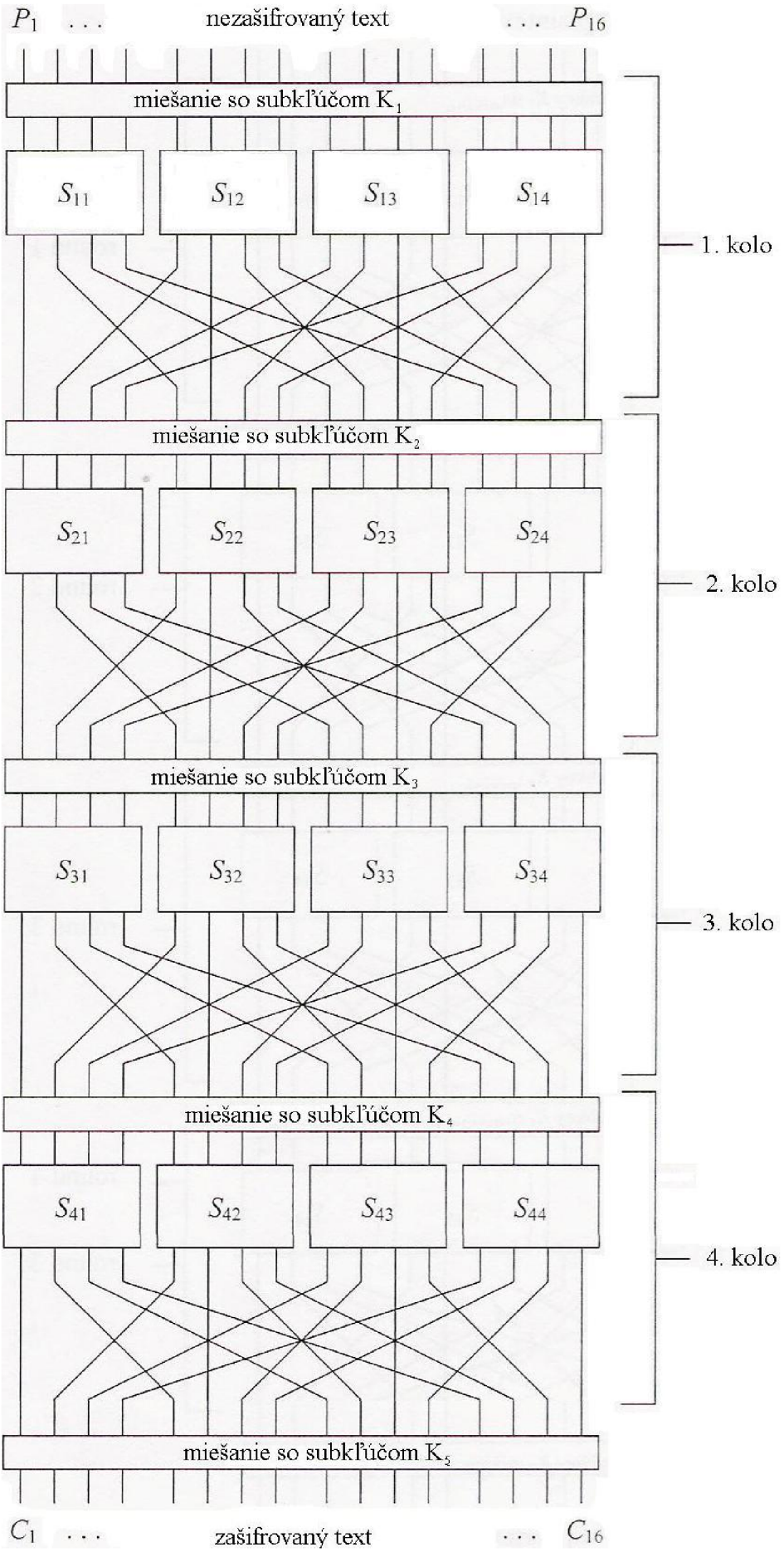
Príloha 1. Substitučno-permutačná šifra – návrh šifry požitej na demonštráciu útoku lineárnou kryptoanalýzou

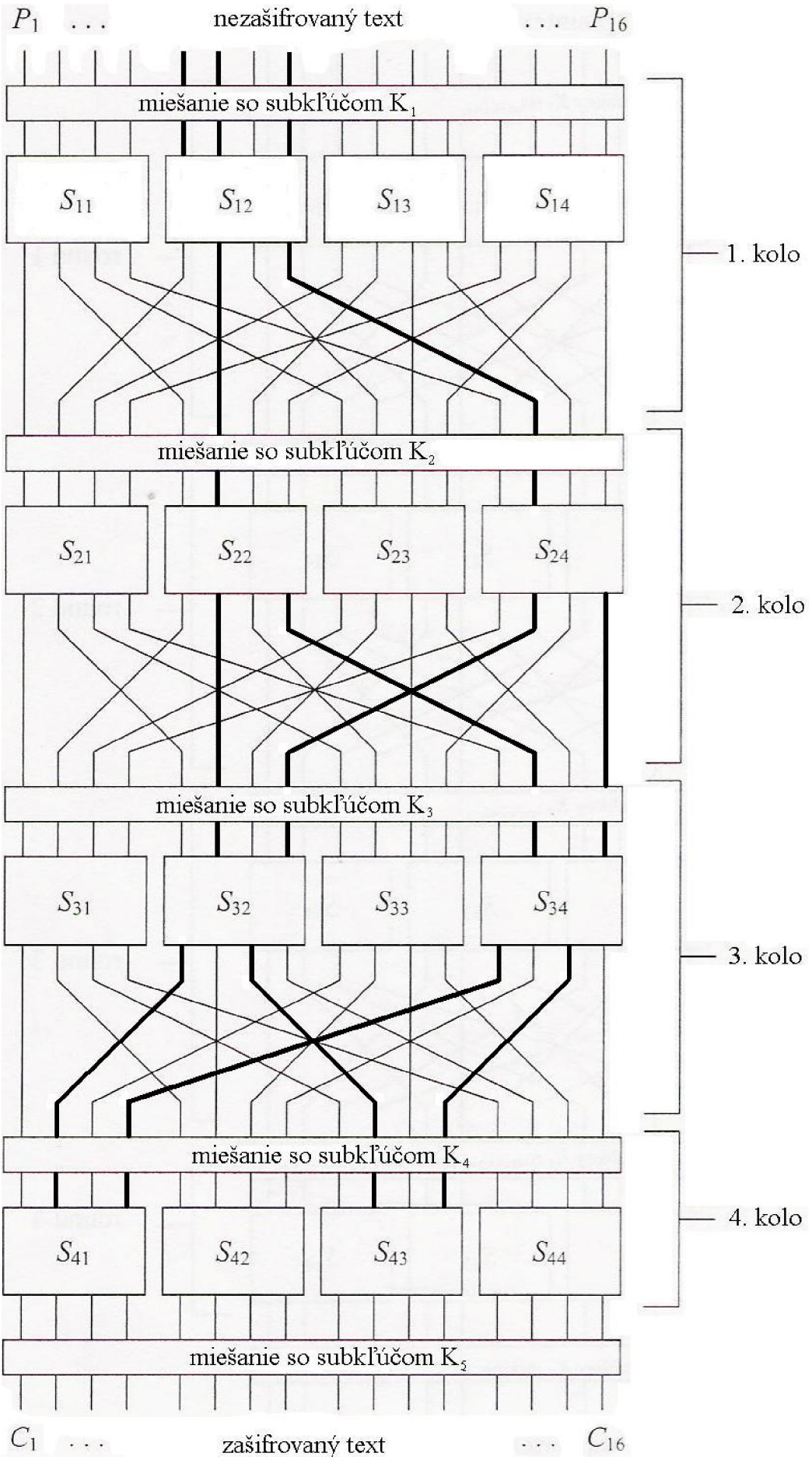
Príloha 2. Substitučno-permutačná šifra – zobrazenie aktívnych S-boxov pri „Aproximácii X“

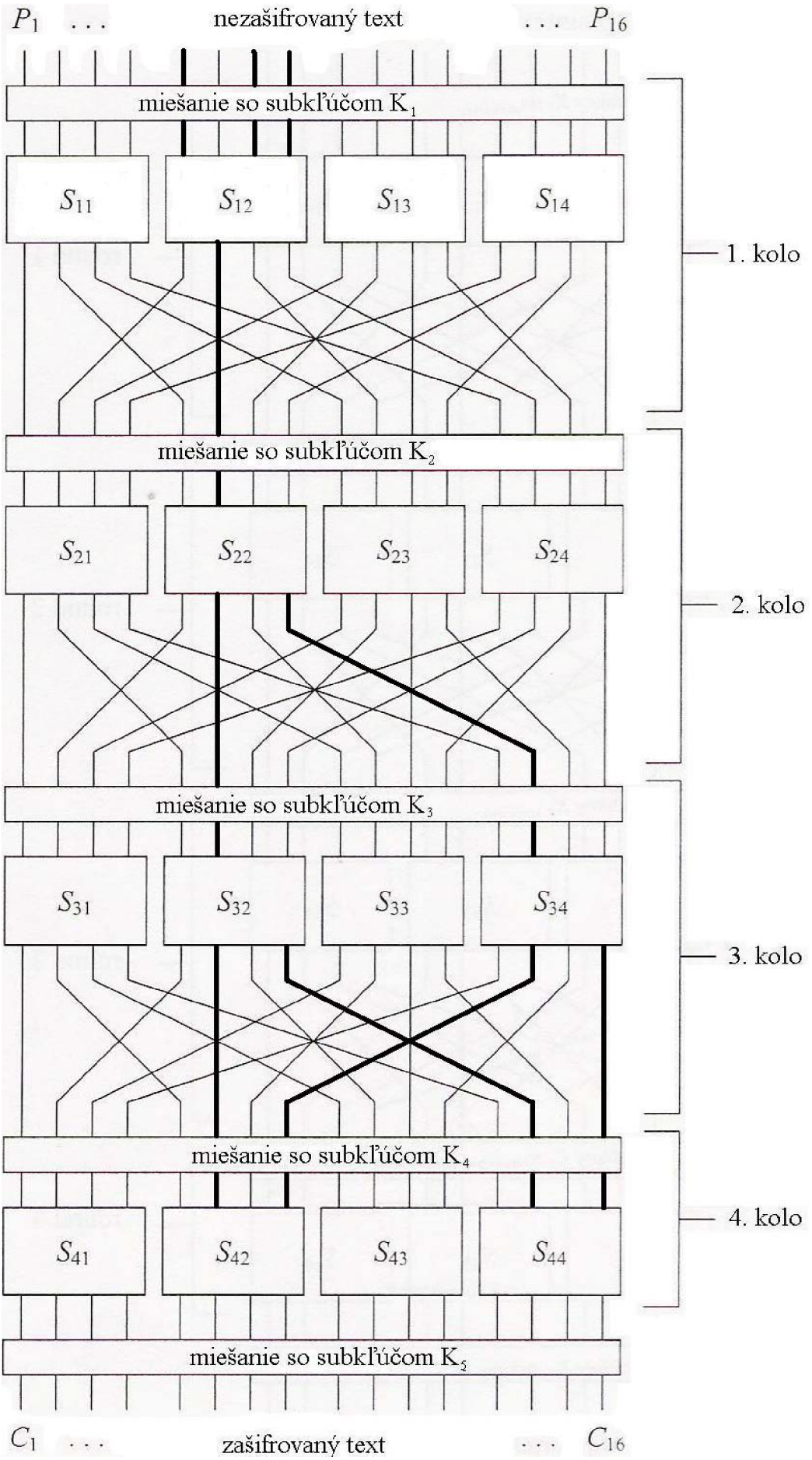
Príloha 3. Substitučno-permutačná šifra – zobrazenie aktívnych S-boxov pri „Aproximácii Y“

Príloha 4. Rozšírený výpis výsledkov útoku

Príloha 5. CD - obsahuje elektronickú formu bakalárskej práce vo formáte PDF, taktiež obsahuje všetky prílohy a obrázky použité v tejto práci ako aj program vytvorený v jazyku C, ktorý bol použitý na simuláciu šifry a k vlastnému útoku na šifru. CD ďalej obsahuje kompletnú tabuľku výsledkov útoku na šifru.


P_1 . . . nezašifrovaný text . . . P_{16}
miešanie so subkľúčom K_1
S_{11} S_{12} S_{13} S_{14}
1. kolo
miešanie so subkľúčom K_2
S_{21} S_{22} S_{23} S_{24}
2. kolo
miešanie so subkľúčom K_3
S_{31} S_{32} S_{33} S_{34}
3. kolo
miešanie so subkľúčom K_4
S_{41} S_{42} S_{43} S_{44}
4. kolo
miešanie so subkľúčom K_5
C_1 . . . zašifrovaný text . . . C_{16}


P1 . . . nezašifrovaný text . . . P16
miešanie so subkľúčom K1
S11 S12 S13 S14
1. kolo
miešanie so subkľúčom K2
S21 S22 S23 S24
2. kolo
miešanie so subkľúčom K3
S31 S32 S33 S34
3. kolo
miešanie so subkľúčom K4
S41 S42 S43 S44
4. kolo
miešanie so subkľúčom K5
C1 . . . zašifrovaný text . . . C16


P_1 . . . nezašifrovaný text . . . P_{16}
miešanie so subkľúčom K_1
S_{11} S_{12} S_{13} S_{14}
1. kolo
miešanie so subkľúčom K_2
S_{21} S_{22} S_{23} S_{24}
2. kolo
miešanie so subkľúčom K_3
S_{31} S_{32} S_{33} S_{34}
3. kolo
miešanie so subkľúčom K_4
S_{41} S_{42} S_{43} S_{44}
4. kolo
miešanie so subkľúčom K_5
C_1 . . . zašifrovaný text . . . C_{16}

1. blok kľúča	3. blok kľúča	počet platných aproximácií	odchylka od 2500		2. blok kľúča	4. blok kľúča	počet platných aproximácií	odchylka od 2500
6	3	2308	192		1	1	2628	128
6	15	2647	147		3	4	2624	124
7	3	2360	140		13	4	2595	95
6	14	2638	138		10	5	2589	89
6	13	2377	123		3	7	2412	88
5	3	2613	113		3	10	2588	88
0	3	2389	111		1	3	2415	85
6	2	2390	110		15	14	2415	85
11	3	2607	107		3	9	2418	82
4	3	2606	106		12	1	2418	82
7	13	2397	103		0	11	2419	81
7	15	2603	103		13	14	2579	79
10	3	2600	100		6	7	2576	76
4	5	2401	99		14	7	2576	76
1	3	2402	98		0	9	2575	75
0	14	2595	95		0	1	2573	73
6	1	2595	95		2	13	2572	72
4	15	2411	89		6	5	2428	72
2	0	2414	86		14	10	2428	72
6	0	2586	86		15	4	2429	71
7	14	2586	86		6	12	2569	69
2	2	2584	84		13	1	2431	69
11	13	2584	84		13	6	2431	69
2	5	2583	83		13	8	2431	69
15	5	2417	83		13	10	2569	69
4	2	2582	82		3	6	2432	68
3	14	2420	80		7	10	2432	68
5	1	2420	80		12	14	2568	68
9	10	2421	79		14	11	2434	66
10	15	2421	79		10	7	2435	65
1	0	2578	78		0	0	2563	63
0	10	2423	77		2	0	2437	63
5	2	2577	77		4	7	2437	63
8	2	2425	75		13	5	2563	63
8	1	2574	74		13	7	2437	63
8	3	2427	73		13	9	2437	63
11	0	2427	73		1	8	2562	62
1	2	2428	72		3	5	2562	62
11	1	2428	72		3	8	2438	62
2	9	2432	68		12	3	2561	61
15	10	2568	68		0	3	2440	60
4	1	2433	67		12	11	2560	60
1	14	2566	66		2	1	2441	59
15	0	2566	66		10	6	2441	59
7	1	2565	65		10	11	2559	59
2	3	2564	64		1	0	2558	58
4	10	2564	64		8	5	2442	58
2	11	2563	63		14	9	2558	58