# Bezpečnost šifry DES

Seminární práce na 4IZ227

Karel Kohout
karel.kohout@centrum.cz, xkohk02
FIS VŠE, 3. ročník

24. dubna 2010

# Obsah



# Seznam tabulek

# Seznam obrázků

# 1 Úvod, vymezení

V práci popisuji teoretické a praktické útoky proti bezpečnosti šifry DES[1]. Mechanismus šifry rozebírám jen na obecné úrovni a v práci neuvádím veškeré potřebné materiály (zejména S-boxy), stejně tak jen okrajově zmiňuji různé módy šifrování, ve kterých je možné DES používat (ECB, CBC, ...) – zvolený mód nijak nezvyšuje bezpečnost samotného algoritmu[2]. Nepopisuji slabiny šifrovacích systému odvozených od DES (zejména TripleDES - 3DES, G-DES, DES-X).

Nejdříve uvádím strukturu šifry na úrovni nezbytné pro popis vybraných možností kryptoanalýzy (tj. vyhýbám se podrobnému popisu rotace klíčů v jednotlivých kolech). Dále zmiňuji některé vlastnosti DES a na konec rozebírám teoretické a praktické útoky proti DES.

# 2 Popis DES

DES je iterativní[3] symetrická[4] bloková šifra pracující s bloky o velikosti 64 bitů a klíčem o velikosti 64 bitů – efektivně 56 bitů, 8 bitů (8., 16., ..., 64.) je určeno pro datovou paritu. Jako standard byla přijata v červenci 1977 ([5], FIPS 46-3[5]), od roku 1999[6] nebylo doporučováno její použití v nových systémech, 25.5.2005 byl oficiálně zrušen standard, ve kterém byla vyhlášena[7]. Vychází z algoritmu Lucifer[8], upraveném NSA[9]. Bezpečnost šifry není založena na skrytí jakékoliv části algoritmu kromě klíče (Kerckhoffův předpoklad). V případě klíče generovaného vhodným (bezpečným) generátorem (pseudo)náhodných čísel implementují klíče nejvýše $2^{56}$ z $2^{64}!$ možných bijekcí na prostoru 64 bitů[10] (v přídadě klíče založeného například na písmenech a číslicích abecedy výrazně méně); při „naivním“ útoku hrubou silou bez další analýzy tedy útočník musí vyzkoušet řádově $2^{55}$ kombinací klíče pro dešifrování zprávy[11].

Při šifrování se nejdříve provede pevně daná permutace (IP[12]) otevřeného textu podle tabulek (provádí se znovu na konci). Poté je z původního klíče $K$ o délce 56 bitů vygenerováno 16 subklíčů $K_i$ o délce 48 bitů a následuje 16 kol tzv. Feistelova schématu. 64 bitů otevřeného textu je rozdělené na dvě poloviny (pravá $R_0$, levá $L_0$). Každé kolo schématu probíhá stejným způsobem. Jako vstup je používány 32bitové řetězce $R_{i-1}$, $L_{i-1}$, ze kterých jsou pro každé i, $1 \leq i \leq 16$, odvozeny $L_i$ a $R_i$ podle následujícího schématu:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i), \text{ kde } f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$$

Vysvětlení: $E$ je pevně daná expanze a permutace $R_{i-1}$ z 32 bitů na 48 bitů (každý bit je použit alespoň jednou, některé dvakrát). $S$ je 8 pevně daných substitucí (*S-boxů*) 6 bitů na 4 bity $S_i$ (pro každé kolo jiné). $P$ je další pevně daná permutace na 32 bitech. Po posledním kole jsou $R_i$ a $L_i$ vyměněny. Dešifrování probíhá stejným způsobem, ale subklíče $K_i$ jsou aplikovány

[1] Data Encryption Standard

[2] Pochopitelně ovlivňuje bezpečnost zprávy delší než je základní blok šifry, ale nikdy nezakryje jakékoliv slabiny v samotném algoritmu.

[3] Tj. vytváří kryptograficky silnou funkcí $n$ iteracemi kryptograficky slabé funkce.

[4] Stejný klíč je použit pro šifrování i dešifrování

[5] Federal Information Processing Standard; jde o třetí revizi – prodloužení.

[6] [5, str. 5]

[7] Federal Register / Vol. 70, No. 96, str. 28907

[8] IBM, Horst Feistel; Lucifer používá bloky a klíč o 128 bitech, je náchylný na diferenční kryptoanalýzu.

[9] National Security Agency

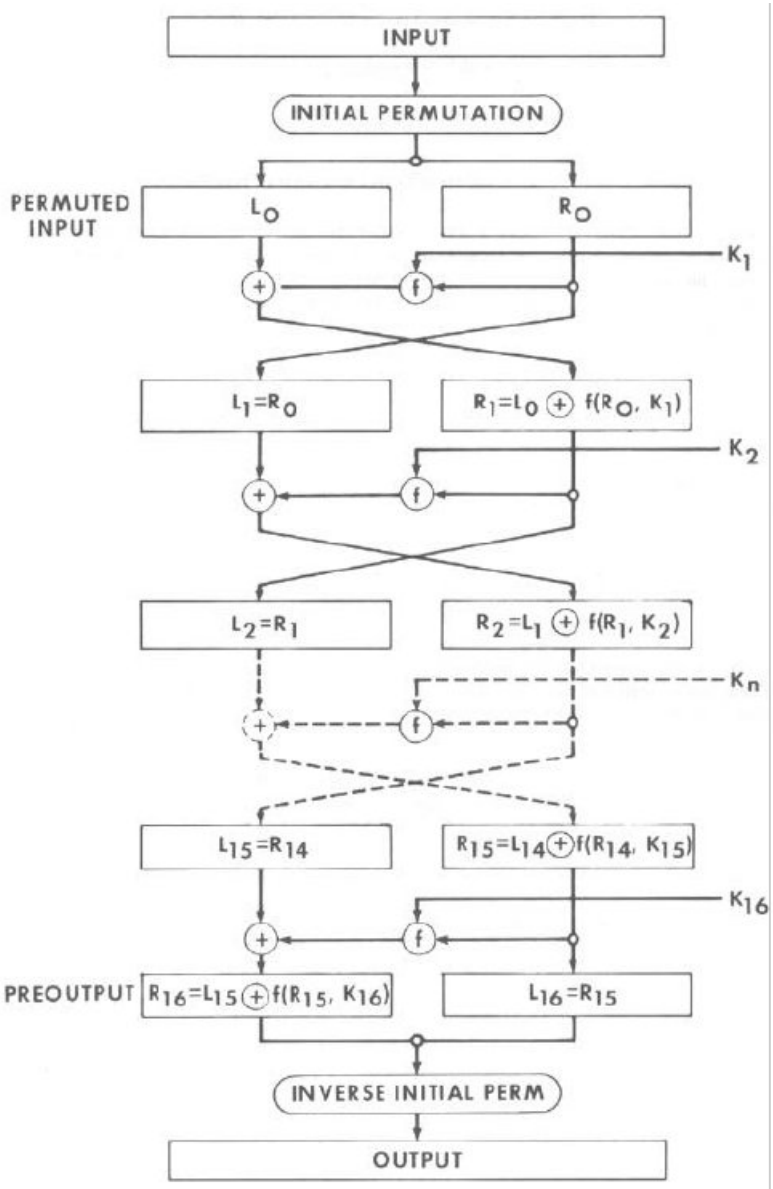
[10] Odvození: [2, str. 252, 7.4.2]

[11] Odvození: [2, str. 233, 7.26]

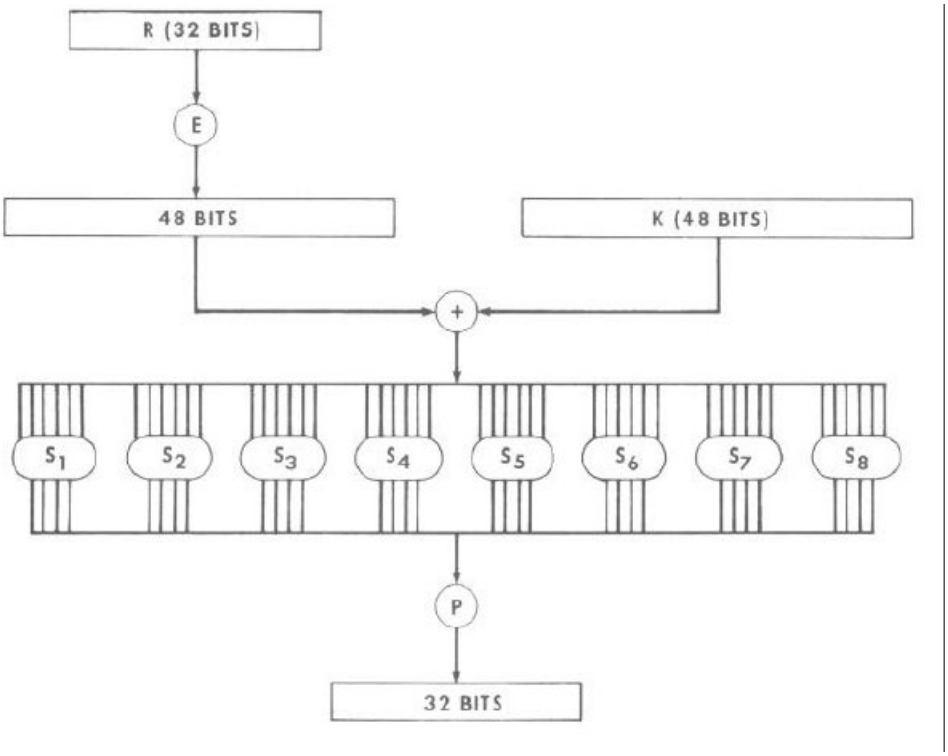
[12] Initial Permutation

v opačném pořadí. Při zjednodušeném vysvětlení je s $R_i$ vždy provedena substituce (závislá na klíči) a následně transpozice.

Klíče $K_i$ jsou odvozeny podle pevně daných permutačních tabulek. Schémata jsou vidět na obrázcích 1 a 2. Tabulky S-boxů a permutací zde neuvádím, protože pro přehled DES nejsou nutné.




Obrázek 1: DES – schéma 16ti kol (zdroj: [5, str. 10])




Obrázek 2: DES – šifrovací funkce kola(zdroj: [5, str. 12])

## 2.1 Vlastnosti a anomálie DES

DES po empirické stránce splňuje předpoklady pro blokové šifry (nebo šifry obecně, viz Shannon): každý bit zašifrovaného textu závisí na všech bitech otevřeného textu (difúze) a všech bitech klíče; neměla by existovat statistická závislost mezi otevřeným a zašifrovaným textem; vztah mezi otevřených textem, zašifrovaným textem a klíčem by neměl být vysledovatelný (zajištěno kombinací lineárních a nelineárních operací – konfúze); změna jednoho bitu otevřeného textu by měla s pravděpodobností 0,5 změnit každý bit zašifrovaného textu; změna zašifrovaného textu by měla způsobit nepředvídatelnou změnu otevřeného textu.

Dále uvádím některé zvláštnosti a výjimky DES, které mohou napomoci kryptoanalýze, případně pomáhají lépe definovat bezpečnost DES. Čerpám z [2], [3], [10] a [4].

**Komplementarita** Nechť $\overline{x}$ je komplementární k $x$. Potom $y = DES_K(x)$ implikuje $\overline{y} = E_{\overline{K}}(\overline{x})$, tj. pokud jsou komplementární klíč $K$ a otevřený text $x$, je komplementární i zašifrovaný text. Komplementárnost běžně nenapomáhá kryptoanalýze při známém otevřeném textu a hledání klíče. Pokud si útočník může zvolit otevřené texty $m_1$, $\overline{m_1}$, může v rámci jednoho zašifrování vyloučit dva potenciální klíče, což snižuje počet očekávaných klíčů z $2^{55}$ na $2^{54}$ (tedy minimálně).

**Slabé klíče** *Slabý klíč* v DES je takový klíč $K$, pro který platí $DES_K(DES_K(x)) = x$; pár částečně slabých klíčů jsou klíče $(K_1, K_2)$ takové, pro které platí $DES_{K_1}(DES_{K_2}(x)) = x$. V DES existují čtyři slabé klíče a šest párů částečně slabých klíčů. Přehled viz [2, str. 258, tabulky 7.5, 7.6].

**DES není grupa (netvoří grupu)[10]** DES definuje množinu permutací zpráv z množiny $M = \{0,1\}^{64}$, kde se permutace sestávají ze šifrování a dešifrování klíči z množiny $K = \{0,1\}^{56}$. Nechť $E_k : M \to M$ je šifrovací permutace pro daný klíč $k$ a $E_k^{-1}$ odpovídající dešifrovací permutace. Pokud by množina permutací DES byla vzhledem ke složenému zobrazení uzavřená (tj. operace šifrování – permutace – uzavřená vzhledem k různým $k \in K$), potom by pro každé dvě permutace $t$, $u$ existovala jiná permutace $v$ taková, že $u(t(m)) = v(m)$ pro každou zprávu $m \in M$. Toto pro DES neplatí, proto opakované šifrování *různými* klíči zvyšuje odolnost vůči luštění.

Vlastnost byla dokázána až v roce 1993, předtím se pouze předpokládala. Opakované šifrování stejným klíčem nemá požadovaný efekt (zvyšuje bezpečnost jen zanedbatelně; efektivní „opakované“ šifrování a dešifrování viz například 3DES).

**Konstrukce S-boxů** Veškeré části DES jsou lineární, až na S-boxy (které do šifry zavádí prvky nelinearity a jsou tudíž naprosto zásadní pro ochranu proti kryptoanalýze vycházející ze známého otevřeného textu). Není známo, jakým způsobem byly S-boxy navrženy – IBM byly dodány z NSA. Panují nepotvrzené předpoklady, že jejich volba může umožňovat kryptoanalýzu šifry (pokud útočník zná jejich konstrukci). Konstrukce a pořadí S-boxů chrání šifru proti diferenční kryptoanalýze (která byla v době návrhu v NSA, ale ne mimo agenturu, do určité míry známa), nikoliv však zcela optimálně.

Dle tvrzení NSA byly S-boxy navrženy podle následujících kritérií:

1. Každý řádek každého S-boxu je permutací čísel $0, \ldots, 15$.
2. Žádný S-box není lineární nebo afinní funkcí svého vstupu.
3. Změna jednoho bitu vstupu do S-boxu způsobí změnu alespoň dvou bitů výstupu.
4. Pro každý S-box a každý vstup $x$ se $S(x)$ a $S(x \oplus 001100)$ liší alespoň o dva bity (velikost $x$ je 6 bitů, vychází z konstrukce S-boxů).
5. $S(x) \neq S(X \oplus 11ef00)$ pro libovolné $e, f$.
6. Je minimalizován rozdíl v počtu nul a jedniček ve výstupu libovolného S-boxu v případě, že jeden z bitů vstupu je konstantní.

Zdroj: [3, kapitola 3.3]; z předchozích čtyř kritérií lze odvodit další dvě; není známo, zda byla při konstrukci S-boxů použita nějaká další.

**Velikost klíče** Samotný klíč DES ($2^{56}$ bitů) byl již v době zavedení standardu považován za velmi malý; je předpoklad, že jeho délka byla snížena úmyslně kvůli snazšímu dešifrování, protože omezení nevychází z technických požadavků a optimalizace průběhu DES pro tehdejší hardware.

# 3 Kryptoanalýza DES

V následující části uvádím známé možnosti kryptoanalýzy šifry DES (lineární, diferenční). Je třeba zdůraznit, že útoky mají teoreticky charakter (vyzkoušení všech klíčů je rychlejší) a předpokládají možnost použít známý otevřený text[13] (nebo otevřené texty). Zároveň jsou zajímavé,

[13]Znalost části otevřeného textu není teoretický předpoklad a je při dešifrování zpráv často používána. U DES může být ztížena vhodným módem se zpětnou vazbou, přesto se některá data dají předvídat. Znalost části obsahu zprávy pomáhala při kryptoanalýze a nalézání denních klíčů například u Enigmy a i u počítačů je možné najít (nebo podvrhnout) opakující se, stereotypní data.

protože poukazují na obecné slabiny blokových šifer (nebo kryptosystémů založených na DES) a výrazně ovlivnily vývoj a konstrukci novějších šifer typu Rijndael (od 2001 jako AES[14]).

## 3.1 Lineární kryptoanalýza

Novější metoda (oproti diferenční, popsané níže); je založena na známém (známých) otevřených textech a statistice[15]. Při dešifrování se pokouší aproximovat nelineární část šifry na lineární rovnici (neboli většinu času je možné získat z lineární rovnice stejné výsledky jako z šifry se zvoleným klíčem). Kvůli pravděpodobnosti je nutné zkoušet velké množství známých otevřených textů, zejména pokud aproximace poskytuje jen mírně lepší výsledek než zcela náhodné „hádání" bitů ($p_0 = \frac{1}{2} = p_1$).

Obecný postup lineární kryptoanalýzy pro Feistelovy šifry je následující:

1. Určení lineární aproximace nelineární části šifry; zaznamenání pravděpodobnosti, s jakou aproximace odpovídá šifře.

2. Rozšíření lineární aproximace na funkci šifry, prováděnou v každém kole (tj. definice lineární rovnice pro každou aproximaci).

3. Konstrukce lineární aproximace celé blokové šifry na základě rovnic pro každé kolo. Pravděpodobnost spolehlivé aproximace lze vypočítat z pravděpodobností aproximací jednotlivých kol.

4. Výpočet potřebného počtu známých otevřených textů pro útok; počet závisí na spolehlivosti aproximace a na minimální požadované pravděpodobnosti úspěchu. Liší se podle typu šifry a velikosti klíče (pro různé klíče může aproximace vycházet s různou přesností).

## 3.2 Diferenční kryptoanalýza

Jde o metodu pracující se známým otevřeným textem. V praxi neumožňuje rozbít všech 16 kol DES, ale pro menší počet kol velmi zjednodušuje nalezení klíče (pro 8 kol otázka minut na běžném počítači). Stručný popis:

Nechť $L_0R_0$ je otevřený text, nechť $0 \leq n \leq 16$ a nechť $L_nR_n$ je zašifrovaný text v n-tém kole (je vynechána permutace IP na začátku a na konci DES, není prováděna inverze DES[16]). Potom spočívá diferenční kryptoanalýza v porovnávání $L_0^{'}R_0^{'}$ ($L_0^{'}R_0^{'} = L_0R_0 \oplus L_0^*R_0^*$, kde $L_0^*R_0^*$ a $L_0R_0$ jsou dva různé otevřené texty) s $L_n^{'}R_n^{'}$ ($L_n^{'}R_n^{'} = L_nR_n \oplus L_n^*R_n^*$). Jinými slovy hledá, jak se projeví rozdíl mezi známým otevřeným textem v zašifrovaném textu.

Mnohem detailnější popis včetně konkrétního příkladu pro DES je v [4]. Pro DES se 16 koly je diferenční kryptoanalýza pomalejší než zkoušení všech klíčů (vyžaduje $2^{58}$ kroků; zdroj: [4]). Z textu Bihama a Shamira vyplývá poměrně důležitý závěr: S-boxy byly skutečně zvoleny tak, aby odolávaly diferenční kryptoanalýze (náhodné S-boxy výrazně zjednodušují rozbíjení kryptosystému; rovněž v rámci S-boxu je třeba jednotlivé substituce vhodně volit tak, aby byl celý S-box odolný vůči diferenční kryptoanalýze nejen v rámci jednoho kola, ale zároveň v rámci více kol a všech kol dohromady). Postup je aplikovatelný i na jiné šifry, podobné DES.

Na závěr ještě poslední slabina: DES s méně koly je náchylný k „meet-in-the-middle" útoku, který pro snížený počet kol DES výrazně snižuje velikost prostoru pro klíč. Tento útok ale není proveditelný pro DES s plnými 16ti koly (ale je proveditelný pro některé šifry podobné DES).

[14] Advanced Encryption Standard; nahradil DES.
[15] Matsui, 50 počítačů, rozbití DES při $2^{43}$ známých otevřených textech.
[16] Žádná z těchto operací nijak zásadně nezvyšuje odolnost DES proti kryptoanalýze.

# 4 Praktické útoky proti DES

Předchozí útoky ukazují na teoretické slabiny DES. Vzhledem k velikosti klíče a rychlosti počítačů je ale pravděpodobné, že pro útoky byla od začátku v praxi používána hrubá síla (předpokládám útoky různých státních institucí s příslušným rozpočtem; prakticky využitelná slabina, která by nebyla založena na útoku hrubou silou, zatím nebyla nalezena). Různými formami jejího nasazení se zabývám v další části práce.

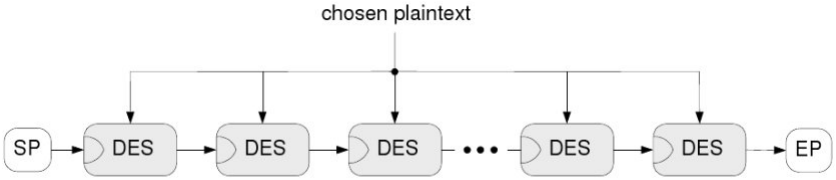
Nejjednodušší útok na DES v případě možnosti volby otevřeného textu je vyzkoušení – vyčerpání všech možností. V průměru je pro nalezení klíče třeba vyzkoušet $2^{55}$ možných kombinací. Při hledání více klíčů a známém otevřeném textu $x$ je vhodné si vytvořit seznam všech možných výsledků $y_K = DES_K(x)$ pro každý možný klíč $K$ ($2^{56}$ kombinací). V takovéto tabulce lze vyhledávat se složitostí $O(n)$ (ovšem na úkor paměťových nároků, potřebné množství paměti je řádově 960 petabajtů). Při hledání více klíčů tabulka zrychluje dešifrování (oproti procházení celého prostoru pro každý klíč zvlášť, jako to dělají „jednorázové“ DES crackery).

Pro DES byl prezentován útok (Hellman) vyvažující potřebný strojový čas a paměť při známém otevřeném textu, který vyžaduje $mt$ slov paměti a $t^2$ operací za předpokladu, že $mt^2$ je rovno počtu možných klíčů ($2^{56}$), jehož variantu popisuji v následující části textu.

## 4.1 Time-memory tradeoff

Kryptoanalýza klíče o délce k bitů má obecně složitost $O(K^{\frac{2}{3}})$ operací (poznámka[17]: $K = 2^k$) a $O(K^{\frac{2}{3}})$ paměti, pokud je před kryptoanalýzou vypočítáno $O(2^k)$ (tedy $K$) operací předem. Pro luštění DES je možné použít několik možných poměrů, jako příklad uvádím metodu používající „distinguished points“ (DP)[18].

**Postup** Je vytvořen řetězec $l$ šifrovacích operací se známým otevřeným textem a $l$ operacemi. Zřetězení je dosaženo přes použití zašifrovaného bloku jako klíče pro další operaci v řetězci (čímž se vytvoří všechny nebo většina možných klíčů[19]). Pro počátek a konec řetězce (DP) platí pevně dané vlastnosti (nedochází tedy při pozdější kontrole k jejich hledání). Při přípravě útoku je předem vypočítáno množství těchto řetězců a jsou uloženy DP a délka řetězce (obrázek 3).




Obrázek 3: Time-memory tradeoff (zdroj: [6, Fig. 1])

Poté při samotném hledání klíče ke známému otevřenému textu ze zašifrovaného lze použít následující postup: zašifrovaný text je použit jako klíč pro otevřený text v řetězci, dokud není nalezen DP (zašifrovaný text s konkrétními vlastnostmi). Následně je prohledán seznam koncových DP; pokud je DP nalezen, pustí celý útočník řetěz od počátečního DP, dokud nenalezne zašifrovaný text. Jeho předek v řetězci je potom klíč použitelný k dešifrování.

[17] Z důvodu čitelnosti.
[18] Český překlad pravděpodobně význačné body?
[19] V [6] autoři uvádí i možnost, kdy klíč není v tabulce nalezen.

Problém metody spočívá kolizích řetězců a pokrytí prostoru klíčů, proto je třeba volit různé funkce pro vypočítání DP (například XOR s pevně daným řetězcem). Implementace je možná hardwarově (tudíž velmi rychle) po úpravě FPGA obvodů a překračuje rozsah této práce, proto ji neuvádím.

V praxi útok používající time-memory tradeoff výrazně snižuje náklady a zvyšuje rychlost nalezení klíče (oproti klasických DES crackerům) a je použitelný i proti mnoha jiným systémům (zejména hash funkce, „rainbow tables“ a spol.) Podle autorů [6] jsou náklady na jednorázové předpočítání řetězců kolem 12 000 USD a týden času, následné nalezené jednoho klíče je možné v řádu desítek minut s jediným FPGA obvodem (12 USD). Pravděpodobně jde o metodu, která by byla použita, pokud by se někdo pokoušel dešifrovat zrávy v masovém měřítku.

## 4.2 DES cracker

První útok hrubou silou teoreticky navrhli Diffie a Hellman (1977[20]) na stroji s $10^6$ DES čipy, cenou 20 milionů USD a očekávanou dobou hledání 12 hodin (tehdy zcela realizovatelné agenturou s velikostí, rozpočtem a znalostmi NSA, ale mimo dosah běžné komerční sféry) – zároveň už zmiňují, že v 90. letech bude DES běžně luštitelný s mnohem menšími rozpočty. V roce 1993 Wiener[21] navrhl „DES cracker“ s 57 600 DES čipy, cenou 1 milion USD[22] a očekávanou dobou běhu 3,5 hodiny.

První efektivní veřejně známé útoky vůči DES byly provedeny právě přes DES crackery. To je dáno zejména návrhem DES (jednoduchá hardwarová implementace, na úrovni software je vždy pomalejší). Jde o hardwarové zařízení, které v rámci velké paralerizace (řádově stovky až tisíce čipů) zkouší všechny možné klíče (prochází celý prostor klíčů). Problém představuje určení, zda skutečně dešifrovaný text odpovídá hledanému – lze kontrolovat buď základě vylučování podle určitých kritérií (u textu bude předpoklad vysokého zastoupení tisknutelných ASCII znaků) nebo (spíš následně u malého procenta textů) na základě určitých předpokladů (u RSA challenge měl výstupní text připomínat anglický jazyk, případně jazyk obecně, což na nejzákladnější úrovni lze kontrolovat přes analýzu koincidencí). Cíl je samozřejmě vyřadit co největší množství zpráv na co nejnižší úrovni a ke zpracování na úrovni software posílat jen zanedbatelné procento.

Liší se útok se známým otevřeným textem (DES cracker šifruje text náhodnými klíči, dokud se „netrefí“) a bez známého otevřeného textu.

Samotné veřejné rozbití DES v praxi bylo podpořeno autory “konkurenčního” algoritmu (RSA Laboratories; byť RSA je založené na principu soukromého a veřejného klíče (Diffie-Hellman) a modulární aritmetice) přes několik soutěží – RSA Challenges.

První (DES-I) byla vyhlášena 28.1. 1997 na RSA Cryptographic Trade Show v San Franciscu, cílem bylo nalézt neznámý otevřený text[23] ze zašifrovaného textu. Úspěšný (v případě DESu) byl projekt DESCHALL (Rocke Verser, Matt Curtin a Justin Dolske), pracující na principu distribuovaných výpočtů přes internet a hrubé síly – v nejhorším případě by bylo třeba vyzkoušet všech $2^{56}$ možných klíčů (úspěšní byli za 96 dnů – 18 června – po prohledání zhruba 25 % možných kombinací [13]). Útok je podstatný kvůli svému principu – možnost masově provádět distribuované výpočty velmi zvyšuje požadavky na odolnost algoritmů[24]. Zároveň byla v soutěži poprvé veřejně předvedena nízká odolnost DES (předtím pouze předpokládaná odbornou veřejností).

[20] W. Diffie, M. Hellman, Exhaustive Cryptanalysis of the NBS Data Encryption Standard, Computer, vol 10, pp 74-84, 1977.

[21] M.J. Wiener, Efficient DES Key Search, Technical Report TR-244, School of Computer Science, Carleton University, Ottawa, 1994

[22] Se započtením inflace mnohem méně než 1 milion v roce 1977

[23] „Strong cryptography makes the world a safer place.“

[24] V dnešní době nemusí jít o dobrovolný projekt – není problém si na výpočty pronajmout určitý počet strojů v rámci botnetu (marketingově „cloud computing“ trochu jinak).

V roce 1998 proběhly dvě kola (DES-II-1, DES-II-2); první začalo 13.1.1998 a skončila 23.2.1998, úspěšnými řešiteli byla skupina `disributed.net` ([12]) za 39 dnů. Druhé kolo bylo vyhlášeno 13. července 1998, správný klíč a otevřený text byl nalezen na specializovaném hardware („Deep Crack“) EFF (Electronic Frontier Foundation) za 39 hodin (14.7.1998). EFF postavila první hardwarový DES cracker nepodléhající utajení za méně než 250 000 USD (1998, neupraveno o inflaci). Třetí soutěž (DES -III) byla vyhlášena 18. ledna 1999, k rozbití kryptogramu došlo za 22 hodin, 16 minut a 4 vteřiny (distributed.net a EFF dohromady).

V současné době je možné DES rozbíjet na stroji se zanedbatelnou cenou kolem 10 000 USD a dobou běhu pod 3 dny [6].

# 5 Závěr

Bloková šifra DES je v dnes již překonaná a neměla by již být používána. Z hlediska standardů je nahrazena AES, v některých oborech jsou však stále nasazeny kryptosystémy vycházející z DES (zejména 3DES – Triple DES) – příkladem je EMV[25] u platebních karet. DES výrazně napomohl rozvoji počítačů a výměny dat – jednalo se o první veřejný standard, oproti kterému bylo možné implementovat kryptografické systémy. Zároveň se na něm ukázaly některé obecné nedostatky, které byly odstraněny až u AES. U DES není možné, na rozdíl od novějších šifer typu Rijndael, matematicky dokázat, že je bezpečný (neznámý původ S-boxů). U novějších šifer jsou voleny výrazně delší klíče, s ohledem na zkušenosti s DES – je předpoklad, že jakýkoliv standard se udrží poměrně dlouhou dobu (25 let u DES) a je proto třeba zakomponovat dostatečnou rezervu bez ohledu na zájmové organizace (NSA), protože jinak dojde k vytváření ne zcela optimálních mezičlánků (3DES, DES-X).

[25] **E**uropay, **M**asterCard and **V**ISA,

# A Rozsah práce

Předpokládám jako požadovaný rozsah 10 normostran (1 NS = 1800 znaků).

| Statistics for xkohk02.tex | |
|---|---|
| Characters | |
| Words and numbers: | 18505 |
| LaTeX commands and environments: | 2055 |
| Punctuation, delimiter and whitespaces: | 5177 |
| Total characters: | 25737 |
| | |
| Strings | |
| Words: | 3394 |
| LaTeX commands: | 240 |
| LaTeX environments: | 12 |
| Total strings: | 3646 |

Poznámka: všechny odkazy byly mezi 12.4.2010 a 25.4.2010 funkční (vzhledem k délce psaní práce neuvádím data u každého odkazu zvlášť). Platí i pro odkazy v textu.

# Reference

[1] Grabbe, J. Orlin, The DES Algorithm Illustrated
http://orlingrabbe.com/des.htm

[2] Menezes, Alfred J., Oorschot, Paul C. van, Vanstone, Scott A.: Handbook of applied cryptography, CRC Press, 1996, ISBN 9780849385230

[3] Stinson, Douglas: Cryptography - Theory and practice, CRC Press, 1995, ISBN: 0849385210

[4] Biham, Eli, Shamir, Adi: Differential Cryptanalysis of DES-like Cryptosystems, 1990
http://www.cs.technion.ac.il/~biham/Reports/Weizmann/cs90-16.ps.gz

[5] U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology: FIPS PUB 46-3 – DATA ENCRYPTION STANDARD (DES), 1999
http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[6] Quisquater, Jean-Jacques, Standaert, François-Xavier: Exhaustive Key Search of the DES: Updates and Refinements, UCL Crypto Group, Laboratoire de Microélectronique, Université Catholique de Louvain
http://www.dice.ucl.ac.be/~fstandae/PUBLIS/28.pdf

[7] Cryptographic Challenges (RSA Laboratories),
http://www.rsa.com/rsalabs/node.asp?id=2091

[8] DESCHALL project,
http://www.interhack.net/projects/deschall/

[9] "EFF DES CRACKER"MACHINE BRINGS HONESTY TO CRYPTO DEBATE, EFF,
http://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_descracker_pressrel.html

[10] Campbell, Keith W., Wiener, Michael J., DES is not a group,
http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C92/512.PDF

[11] Klíma, Vlastimil, Základy moderní kryptologie - Symetrická kryptografie II.
http://crypto-world.info/klima/mffuk/Symetricka_kryptografie_II_2006.pdf

[12] distributed.net mailing list, 24 Feb 1998 23:38:58 -0600, Subject: [RC5] [ADMIN] The secret message is...
http://www.distributed.net/pressroom/news-19980224.txt

[13] DES Encryption Challenge
http://gilchrist.ca/jeff/distrib-des.html