EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Kryptologie

Kryptoanalýza a základní útoky na šifry

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204

Doc. Ing. Roman Šenkeřík, Ph.D.
FAI, Ústav informatiky a umělé inteligence

Obsah prezentace

- Kryptoanalýza – úvod a rozdělení
- Základní (nejčastější) útoky na šifry
- Fyzické limity a další souvislosti

1. Kryptoanalýza

Kryptoanalytické techniky - obecné rozdělení

- Metoda pokus-omyl
- U klasických šifer frekvenční analýza (rozhodnutí zda se jedná o substituci či transpozici - v případě substituce vede k rozluštění.
- Luštění transpozic v tabulce - postupné přeskupování bloků (sloupce atd) v tabulce a vyhledávání bigramů a trigramů (častých pro konkrétní jazyk)
- Luštění polyalfabetických šifer - algoritmus založen na výskytu stejných dvojic OT a klíče - matematická analýza, tzv. index koincience

Kryptoanalytické techniky - obecné rozdělení

- Slovníková metoda hledání klíče (Dictionary Brite Force attack)
- Brute force attack - útok hrubou silou, zkoušení všech permutací/variací klíče
- Lineární kryptoanalýza
- Diferenciální kryptoanalýza

Kryptoanalytické techniky: detailní rozdělení (z pohledu způsobu luštění)

- Luštění se znalostí šifrového textu (Ciphertext-only attack)
- Luštění se znalostí otevřeného textu (Known-plaintext attack)
- Luštění s možností volby otevřených textů (Chosen-plaintext attack)

Kryptoanalytické techniky: detailní rozdělení (z pohledu způsobu luštění)

- Adaptivní metoda luštění s možností volby otevřených textů (Adaptive - Chosen-plaintext attack)
- Luštění s možností volby šifrových textů (Chosen-ciphertext attack)
- Luštění s možností volby vybraného klíče (Chosen-key attack)

Kryptoanalytické techniky: detailní rozdělení (z pohledu způsobu luštění)

- Útok hrubou silou (Brute force attack).
- Útok postranními kanály (Side channel attack).
- Agenturní, korupční kryptoanalýza (Agency/Purchase-key Attack).
- Pendreková Analýza (Rubber-hose attack).

2. Útoky na šifrovací systémy

Luštění se znalostí šifrového textu (Ciphertext-only attack)

- Nejzákladnější a bohužel (bohudík) nejčastější a nejtěžší forma.

- Je k dispozici šifrový text několika zpráv, které byly zašifrovány stejným šifrovacím algoritmem.

Luštění se znalostí šifrového textu (Ciphertext-only attack)

- Úkolem je odvodit co nejvíce Otevřených textů nebo úplně nejlépe klíč (nebo klíče) použité k zašifrování. Tím pádem možno dešifrovat jiné zprávy od stejného odesílatele/příjemce za předpokladu, že byl použit stejný algoritmus a klíč nebo odhalená množina klíčů

- Šifrovací systém, který lze tímto způsobem prolomit za “rozumnou dobu” by neměl být používán! [1]

Luštění se znalostí otevřeného textu (Known-plaintext attack)

- Je k dispozici zašifrovaný text (texty), ale i odpovídající otevřený text (texty).
- Úkolem je odvodit klíč použitý k zašifrování a tím pádem možno dešifrovat další zprávy od stejného odesílatele/příjemce za předpokladu, že byl použit stejný klíč do doby než bude změněn.
- Nebo je úkolem odvodit algoritmus pro dešifrování všech dalších nových zpráv zašifrovaných stejným klíčem.

Luštění se znalostí otevřeného textu (Known-plaintext attack)

- Toto může nastat pokud je identická zpráva zašifrována jednak pomocí nového systému a jednak starým systémem, který již kryptoanalytik umí luštit.

- A nebo dojde k získání několika dešifrovaných textů, jejichž odpovídající šifrové texty byly zachyceny a je možné je “zpárovat”

- Tento útok je proveditelný většinou v situacích, kdy došlo k hrubému porušení kryptografických pravidel. [1]

Luštění s možností volby otevřených textů (Chosen-plaintext attack)

- Je k dispozici zašifrovaný text (texty), ale i odpovídající otevřený text (texty), navíc si Kryptoanalytik vybírá otevřené texty (výběrové bloky), které šifruje.

- Úkolem je odvodit klíč použitý k zašifrování a tím pádem možno dešifrovat další zprávy od stejného odesílatele/příjemce za předpokladu, že byl použit stejný klíč do doby než bude změněn.

- Výhodnější než předchozí způsob, šifrováním zvolených krátkých textů (bloků) je možno získat více možných informací o klíči a vodítek k jeho získání.

Luštění s možností volby otevřených textů (Chosen-plaintext attack)

- Někdy jsou voleny jen velmi krátké texty, jež jsou zašifrovány - plaintext injection attack.

- Tímto útokem je velmi ohrožena asymetrická kryptografie - veřejný klíč je běžně k dispozici a tak případný útočník může zkoušet šifrovat obrovské množství různých krátkých vzorových textů a získat tím odpovídající zašifrované texty. [1]

Adaptivní metoda s možností volby otevřených textů (Adaptive - Chosen-plaintext attack)

- Založeno na minulém typu útoku
- Výběr otevřeného textu je ovlivněn předchozím výsledkem pokusného šifrování (adaptivita).
- Šifrovací systémy, které jsou odolné tomuto typu útoku lze považovat za velmi silné [1].

Luštění s možností volby šifrových textů (Chosen-ciphertext attack)

- Jsou k dispozici zašifrované texty, a Kryptoanalytik si je libovolně může dešifrovat a má přístup ke vzniklým otevřeným textům.

- Úkolem je odvodit klíč použitý k zašifrování a tím pádem možno dešifrovat další zprávy od stejného odesílatele/příjemce za předpokladu, že byl použit stejný klíč do doby než bude změněn.

- Útok je proveditelný v situaci, kdy má Kryptoanalytik přístup ke kryptografickému zařízení (algoritmu), které umí dešifrovat vložený text [1].

Luštění s možností volby vybraného klíče (Chosen-key attack)

- Málo známa a těžce aplikovatelná metoda

- Využití určitých vztahů (pokud existují) mezi jednotlivými klíči [1].

Útok hrubou silou (Brute force attack)

- Analytický test pro vyzkoušení všech možných nastavení klíče a vyhodnocení, zda byl nalezen ten správný.

- Je to vždy útok se znalostí otevřeného textu - Known-plaintext-attack!

- Musím znát alespoň nějakou část otevřeného textu, nebo jeho strukturu, aby bylo možno provést test a vyhodnocení (předem známá část OT - oslovení, příkaz, místo určení, kontaktní údaje, kód odesilatele, typ souboru získaný z hlavičky, CRC součet pro archívy (rar, zip), atd...

Útok hrubou silou (Brute force attack)

- Teoreticky vždy úspěšný postup (kromě Vernamovy šifry), ale prakticky proveditelný jen pro malé množství klíčů.
- Existují modifikace - slovníkový útok hrubou silou - vyzkoušení všech možných klíčů ze “slovníku” nejčastěji používaných klíčů a jejich kombinací.
- Nebo například klíč se může skládat z více částí - některé jsou úspěšně odhadnuty, jiné dohledány touto metodou. [1]

Útok postranními kanály (Side channel attack)

- Útok veden za účelem získání otevřeného textu nebo klíče.
- Útok postaven proti konkrétním fyzickým realizacím šifrovacích systémů.
- Založený na principu, že fyzická reallizace šifrovacího algoritmu, je vždy odlišná od matematické abstraktní teorie.

Útok postranními kanály (Side channel attack)

- Analýza možných úniků informací při elektromagnetickém vyzařování, měření spotřeby energie, času...
- Využití řady jiných senzorů, kamer, snímání odlišných zvuků při stisku jednotlivých kláves, atd…
- Existují řada dalších charakteristik, podle kterých se dá na první pohled kvalitní a vysoce odolný šifrovací systém degradovat na lehce překonatelný. [1]

Agenturní, korupční kryptoanalýza (Agency/Purchase-key Attack)

- Útok veden za účelem získání klíče nebo dalších údajů k šifrovacímu systému.
- Útok postaven na metodách sociálního inženýrství/phishing/pharming.
- Založený na principu získání informací od osob, jež ani netuší, že předaly citlivé informace nebo došlo k předáním informacím osobám, jež se vydávaly za důvěryhodné.
- Využití i klasických “agenturních” metod - krádež, ofocení, opis... [1]

Pendreková Analýza (Rubber-hose attack)

- Nejstarší a “nejúčinnější” metoda.
- Útok hrubou (ale fyzickou) silou.
- Založený na principu získání informací o šifrovacím systému od osob, jež jsou mučeny, vydírány, fyzicky napadány, atd... [1]

Kryptoanalýza monoalfabetických substitučních šifer

- Je založena na vlastnostech jazyka.
  - Primárně je založena na analýze četnosti výskytu jednotlivých znaků neboli frekvenční analýze. Při substituci totiž dochází k přímému přenesení statistických vlastností abecedy otevřeného textu na abecedu šifrového textu.
  - Dále spočívá ve vyhledávání typických shluků znaků pro daný jazyk (bigramy, trigramy), typických prvních / posledních znaků slov, ověřování poměru samohlásek a souhlásek, atd…

Kryptoanalýza monoalfabetických substitučních šifer [1]

- Pořadí hlásek v češtině:
  - E,O,A,I,N,S,T,R,V,U,L,Z,D,K,P,M,C,Y,H,J,B,G,F,X,W,Q
- Pořadí hlásek v češtině na začátku slov:
  - P,S,V,Z,N,T,O,J,K,D,A,B,M,R,U,C,I,H,E,L,F,G,W,Y,Q,X
- Pořadí hlásek v češtině na konci slov:
  - E,I,A,O,U,Y,M,T,H,V,L,K,S,Z,D,N,R,C,J,B,P,G,F,W,X,Q
- Bigramy ST, PR, SK, CH, DN, TR

Kryptoanalýza monoalfabetických substitučních šifer - český jazyk [1]

- Zvláštnosti souhláskových bigramů v češtině:

- ST: S a T má přibližně stejnou frekvenci existuje i bigram TS. Je součástí velkého počtu souhláskových trigramů (STR, STN, STL, STV) vyskytuje se uprostřed i na konci slova.

- PR: P má asi poloviční frekvenci než R. Obrácený bigram RP se téměř nevyskytuje (chrpa). Zpravidla nelze rozšířit „dozadu“ na souhláskový trigram (PRV). Lze rozšířit dopředu na samohláskový trigram (SPR, ZPR,…). Zpravidla stojí na počátku slov.

Kryptoanalýza monoalfabetických substitučních šifer - český jazyk [1]

- CH: H má jen o něco menší frekvenci než C(u kratších textů nemusí platit). Bývá zpravidla na konci slov spolu se samohláskami Y,I,A,E (YCH, ICH, ACH, ECH) Většinou platí: předchází-li CH souhláska, pak je po něm samohláska a naopak (OBCHOD, NECHŤ).

- Trigramy: PRO, UNI, OST, STA, ANI, OVA, YCH, STI, PRI, PRE, OJE, REN, IST, STR (nejběžnější souhláskový trigram!), EHO, TER, RED, ICH.

Kryptoanalýza polyalfabetických substitučních šifer

- Základem je určení počtu použitých substitucí, dále dokument rozdělíme na části, šifrované stejnou substitucí a na tyto části použijeme postupy analýzy monoalfabetických šifer. Metody určování počtu použitých substitucí [2] :

- **Kasiského metoda**
  - Pokud se v otevřeném textu vyskytuje k-krát stejný řetězec znaků a k šifrování bylo použito n substitucí, které se cyklicky střídají, bude daný řetězec zašifrován přibližně k/n krát stejně. Prohledáváme zašifrovaný text na výskyt opakujících se řetězců (délky aspoň 3). Zjistíme vzdálenosti začátků jednotlivých řetězců. Ke každé vzdálenosti získané v předchozím bodě vytvoříme seznam všech dělitelů tohoto čísla. Počet použitých substitucí by měl odpovídat některému z často se vyskytujících dělitelů.

Kryptoanalýza polyalfabetických substitučních šifer

- **Index koincidence**
  - Index koincidence je hodnota, která může pomoci rozhodnout, zda byla pro zašifrování textu použita monoalfabetická či polyalfabetická šifra. Je-li text zašifrován monoalfabetickou šifrou, měl by se jeho index koincidence blížit indexu koincidence jazyka, ve kterém byl napsán. Je-li text zašifrován polyalfabetickou sifrou, bude se jeho index koincidence blížit indexu koincidence náhodně generovaného jazyka [2]. A zároveň se jedná o pravděpodobnost, že ve dvou různých textech se na jednom miste objeví stejný znak.
  - Pokud má odpovídající otevřený text rozložení znaků blízké normálu, lze z IC usuzovat na počet použitých substitucí. Složitost analýzy polyalfabetických šifer roste s počtem použitých substitucí (délkou klíče).
  - Pěkný příklad: [2].

Kryptoanalýza transpozičních šifer

- **Jednoduchá transpozice.**
  - Je-li k dispozici pouze jeden šifrový text dané délky, nezbývá než jej přehazovat za použití častých bigramů tak, aby se dostal smysluplný text.
  - Je-li k dispozici více textů téže délky zašifrované stejnou permutací, pak jsou napsány pod sebe, rozstříženy do sloupců a přeházeny opět tak, aby se ve všech řádcích současně dostaly smysluplné texty [1].

Kryptoanalýza transpozičních šifer

- **Transpozice s klíčem:**
  - V tomto případě se může rozměr tabulky najít tak, že se vyzkouší všechny možné tabulky, které lze celé vyplnit šifrovým textem dané délky. Pro každou možnost je spočítáno poměr samohlásek a souhlásek v jednotlivých řádcích.
  - Tabulka, pro kterou se tyto poměry nejvíce blíží poměru samohlásek a souhlásek v přirozeném jazyce otevřeného textu, je ta nejpravděpodobnější.
  - Text si potom rozstříhán do sloupců a pokračuje se stejně jako u více textů téže délky [1].

Diferenciální Kryptoanalýza - Popis

- Blokové symetrické šifry pracují na principu substituce a permutace nad blokem dat v několika úrovních (iteracích šifry).
- Šifrování jednoho bloku dat se provádí tak, že v prvním kole se provede substituce podle předpisu, který je realizován tzv. S-boxem (vyhledávací tabulka), poté se provede permutace dat v bloku přehozením pořadí bitů a sloučení s klíčem, nejčastěji operací XOR. Výsledný blok tvoří vstup dalšího kola a postup se opakuje.
- Aplikace S-boxu je jediná operace vnášející nelinearitu.
- Při kryptoanalýze je třeba nelinearitu nějakým způsobem eliminovat.

Diferenciální Kryptoanalýza - Popis

- Diferenciální kryptoanalýza hledá nejvyšší pravděpodobnost výskytu diference výstupu na diferenci vstupu pro všechny dvojice vstupů s konstantním rozdílem.
- Diferenciální analýza je útok se zvoleným textem což znamená, že útočník zná šifrovaný text a odpovídající otevřený (nešifrovaný) text, který si mohl zvolit a snaží se zjistit klíč [1].
- Tato metoda je statistická analýza rozdílů v OT párech a v jejich příslušných šifrových textech. Umožňuje stanovit pravděpodobnost různých klíčů v závislosti na těchto rozdílech a určit tak nejpravděpodobnější klíč.
- Vyžaduje provést analýzu S-boxu dané šifry

Další zajímavosti

- Dříve se věřilo, že smysl kryptologie leží v utajení principu šifrování, dnes je tomu naopak, zveřejňování kryptologických technik má velkou výhodu - zkoušení od nezávislých uživatelů, zkoumání principů více analytiky či amatéry vede k odhalení skrytých chyb, slabin šifry atd...

- I v dnešní moderní době se stále využívá klasických jednoduchých technik

3. Limity útoků a další souvislosti

Další kryptologické zajímavosti

- Steganografie je též velmi často zastoupena v praxi a velmi intenzivně se pracuje na odhalování steganografie.
- Cílem je vývoj sofistikovaných steganofiltrů, např. pro emailovou komunikaci
- Vyšší bezpečnost by mohla být zajištěna tzv superpozicemi šifer - tj n-násobného použití různých technik, nicméně příliš se nepoužívá (výpočetní nároky, řetězení chyb).

Délka klíče (bitová bezpečnost) vs. Kvantové počítače

- Z **Mooreova zákona** [3] vyplývá, že výpočetní výkon se zdvojnásobí zhruba za každých 18 až 24 měsíců, ale i tímto zdvojnásobením jsou v současnosti delší symetrické klíče považovány za bezpečné a mimo dosah [4].

- V dohledné budoucnosti je možnost projít všechny možné 128-bit klíče v konvenční digitální výpočetní technice považováno za nemožné. Nicméně se předpokládají alternativní formy výpočetní techniky, které mohou mít vyšší výpočetní výkon než klasické počítače [4].

Délka klíče vs. Kvantové počítače

- Bude-li k dispozici dostatečné množství spolehlivých kvantových počítačů, je možné snížit 128-bitový klíč až na 64-bitový (z pohledu odolnosti vůči útoku hrubou silou), což je zhruba ekvivalent DES. To je jeden z důvodů, proč AES podporuje 256-bitovou délku klíče [4].

- v roce 1996 bylo matematicky prokázáno, že za přítomnosti velkého množství kvantových počítačů n-bitový klíč může zajistit nejvýše n / 2 bity bezpečnosti. Před kvantovým útokem hrubou silou je snadnější se ubránit tím, že zdvojnásobíme délku klíče, který má malou extra výpočetní hodnotu v běžném používání. Z toho vyplývá, že je vyžadován alespoň 160-bit symetrický klíč pro dosažení 80-bitové bezpečnosti před kvantovými počítači [4].

Délka klíče vs. Kvantové počítače

- Pozor na Asymetrickou kryptografii - ta balancuje na špičce ostří - Existují dva nejznámější útoky kvantové výpočetní techniky založeny na Shorově a Groverově algoritmu. Tyto speciální algoritmy vyvinuté pro řešení kvantových úloh představují velké riziko pro aktuální bezpečnostní systémy postavených na algoritmech s veřejnými klíči jako jsou například RSA, Diffie-Hellman a kryptografie eliptických křivek.
- Citace profesora Gilles Brassarda, který je expertem kvantové techniky: „*Čas potřebný k faktorizaci RSA čísla je stejný jako čas potřebný k použití stejného čísla jako modul pro jedno RSA šifrování. Jinými slovy, netrvá déle prolomit RSA na kvantovém počítači (až na násobnou konstantu), než ho použít na obyčejném počítači.* [4]“

Další zajímavosti

Termodynamické hranice pro útok hrubou silou [1]

- Uvažujme kvantový počítač...

- Dle kvantování energie, která je popsána Planckovou konstantou *k* a absolutní teplotou *T*, je energie nutná pro změnu jednoho bitu minimálně rovna součinu *k*T*. (Minimální množství energie které může být přenášeno při dané teplotě - prakticky to tedy bude asi více).

Další zajímavosti

Termodynamické hranice pro útok hrubou silou [1]

- Teplota pozadí vesmíru je 3,2 *K*, pak ke změně jednoho bitu je nutná energie $4{,}4.10^{-23}$ J.
- Slunce vyzáří za rok energii $1.21.10^{34}$ J.
- Pokud bychom mohli získat veškerou energii Slunce, a kvantový stroj by počítal ve Vesmíru (nebo alespoň na Zemi, ale při teplotě pozadí Vesmíru), teoreticky by tedy bylo možno za rok realizovat $2{,}7.10^{56}$ bitových změn, což přibližně odpovídá vyzkoušení všech možností pro 187 bitový klíč ($2^{187} = 1{,}96.10^{56}$).

Další zajímavosti

Termodynamické hranice pro útok hrubou silou [1]

- Při výbuchu supernovy se uvolní energie, jež by nám mohla pomoci vyzkoušet všechny možnosti pro 219 bitový klíč.
- Je tedy považováno za nemožné “prolomit” 256 bitový klíč.
- (Nemáme dostatek času při použití “přijatelného” množství energie, nebo dostatek energie pro “přijatelný” čas)

Seznam odkazů

[1] VONDRUŠKA, Pavel. Kryptologie, šifrování a tajná písma. Ilustroval Bára BUCHALOVÁ. Praha: Albatros, 2006. Oko (Albatros). ISBN 80-00-01888-8.

[2] Základy kryptoanalýzy. [online]. Dostupné z: http://kix.fsv.cvut.cz/~vanicek/vyuka_l05/kos2.htm

[3] Moorův zákon. [online]. Dostupné z: https://cs.wikipedia.org/wiki/Moor%C5%AFv_z%C3%A1kon

[4] Délka klíče. [online]. Dostupné z: https://cs.wikipedia.org/wiki/D%C3%A9lka_kl%C3%AD%C4%8De

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Děkuji za pozornost

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204