Západočeská univerzita v Plzni

Bezpečnost v informačních technologiích

KIV/BIT

Dokumentace semestrální práce

Vojtěch Danišík
A16B0019P
danisik@students.zcu.cz

14. května 2019

Obsah

1 Zadání **2**

2 Analýza problému **2**

3 Symetrické šifry **2**
3.1 DES 2
3.1.1 Popis 2
3.1.2 Prolomení 3
3.1.3 Závěr 4
3.2 IDEA 4
3.2.1 Popis 4
3.2.2 Prolomení 4
3.2.3 Závěr 5
3.3 AES 5
3.3.1 Popis 5
3.3.2 Prolomení 5
3.3.3 Závěr 6

4 Asymetrické šifry **6**
4.1 RSA 6
4.1.1 Popis 6
4.1.2 Prolomení 6
4.2 ElGamal 7
4.2.1 Popis 7
4.2.2 Prolomení 7
4.2.3 Závěr 8

5 WiFi šifry **8**
5.1 WEP 8
5.1.1 Popis 8
5.1.2 Prolomení 8
5.1.3 Závěr 8
5.2 WPA1/WPA2 8
5.2.1 Popis 8
5.2.2 Prolomení 8
5.2.3 Závěr 8

6 Závěr **8**

1 Zadání

Popis bezpečnosti vybraných šifer a jejich prolamování pomocí vybraných útoků.

2 Analýza problému

Aby bylo možné bezpečně uchovat či poslat důležitá data, tak je potřeba tyto data uložit do formy, ze které by případný útočník nedokázal zjistit obsah dat. Existují dvě hlavní vědní disciplíny, které tento úkol dokáží splnit. První z nich je steganografie, která má za úkol utajit existenci dat (například přepsání nejméně důležitých bitů v obrázku, data rozložena na písmena, která se vyskytují na druhé pozici v každém slově nově vytvořené věty aj.). Druhá z nich je kryptografie, která vstupní data zašifruje do nečitelné podoby pomocí šifrovacích algoritmů. Jelikož výkon počítačů raketově vzrůstá, tak se dost často stává, že starší šifrovací algoritmy jsou prolamovány v relativné krátkém čase (5 hodin, 1 den atp.). Z tohoto důvodu je nutné vynalézat nové a účinější šifrovací algoritmy, které "nebude"možno prolomit v reálném čase. V kapitolách 3, 4 a 5 jsou popsány mnou vybrané šifrovací algoritmy. Některé šifrovací algoritmy jsou již prolomeny a již se ve většině případů nepoužívají, nebo stále používané algoritmy, které ještě nebyly úplně prolomeny.

3 Symetrické šifry

Symetrické šifry používají pro zašifrování i dešifrování stejný klíč. Zašifrovaná data nesmí být dešifrována bez znalosti klíče i v případě, že útočník zná typ použitého šifrovacího algoritmu. Do této dokumentace jsem vypsal 3 z nejznámějších symetrických šifer(DES, IDEA, AES).

3.1 DES

3.1.1 Popis

Data Encryption Standard (DES) je symetrická šifra vyvinutá v 70. letech vědci z firmy IBM. DES se skládá z 16 iterací na základě feistlově síti, kdy ke každé iteraci se využívá podklíč o velikosti 48 bitů, který se liší v každé iteraci. Každý blok je velký 64 bitů, klíč je velký 56 bitů.

3.1.2 Prolomení

Již od vytvoření DESu se vědělo, že algortimus obsahuje bezpečnostní slabiny (například v prvotní implementaci se klíč v části S-box nevolil náhodně). Dnes lze DES prolomit Brute-force (hrubou sílou) útokem již za méně než 24 hodin, což je velice krátká doba. Brute-force útok je takový útok, který se v kryptoanalýze snaží o rozluštění šifry bez znalosti dešifrovacího klíče. V praxi se jedná o systematické testování všech možností (nebo omezené podmnožiny) všech možných kombinací. Čas potřebný pro útok roste exponenciálně s rostoucí délkou klíče.

Existují však i rychlejší varianty prolomení této šifry:

- **Diferenciální kryptoanalýza (DC)** – Diferenciální kryptoanalýzu lze považovat za **chosen plaintext attack**, jejíž útok spočívá v zjištění výsledného zašifrovaného textu pro množinu vstupních dat. Pomocí rozšíření lze dosáhnout i útoků **known plaintext attack** nebo **ciphertext-only attack**. V těchto případech se vypočítá *difference*, která se dá vypočítat mnoha způsoby (nejznámější je využití logické operace XOR). Na základě difference se vypočítá *differential* (pár differencí), které jsou následně analyzovány útočníkem.
  - **Chosen-plaintext attack (CPA)** – Útok se zakládá na náhodném výběru vstupních dat, které se pomocí šifrovacího algoritmu zašifrují a výsledná data jsou použita pro zjištění případných slabin šifrovacího algoritmu. Útok se dá dále rozdělit na dvě skupiny: **Batch/Adaptive chosen-plaintext attack**. **Batch** je neprofesiální, protože útočník si nejdřívě vybere celou skupinu vstupních dat a poté až šifruje. **Adaptive** je profesionální, protože útočník na samém začátku vybere část vstupních dat, které nechá zašifrovat. Po zašifrování vybírá další menší skupinu vstupních dat na základe výsledků šifrování dat předchozích. Pokud je daná šifra odolná proti chosen-plaintext útoku, je zároveň i odolná proti **Known-plaintext** a **Ciphertext-only** útoku.
  - **Known-plaintext attack (KPA)** – Útočník využívající tento útok má přístup jak ke vstupním datům (také nazýváno jako *crib*, slangový výraz pro podvádění), tak i k zašifrovaným vstupním datům. Protože útočník zná jak vstup, tak i výstup, lze pomocí nich zjistit dešifrovací klíč/číselník.
  - **Ciphertext-only attack (COA)** – Jinak nazývaný **known-ciphertext attack**, je útok, kde útočník má přístup pouze k zašifrovaným datům a dokáže podle nich zjistit (vydedukovat, extrahovat) co nejvíce vstupních dat pro zjištění šifrovacího klíče.

- **Lineární kryptoanalýza (LC)** – Lineární kryptoanalýzu lze považovat za **known-plaintext attack**. Útok spočívá ve studování lineárních aproximací mezi paritními bity vstupních dat, zašifrovaných dat a neznámého klíče.

- **Daviesův útok** – Daviesův útok byl vytvořen Donaldem Daviesem v roce 1987 (v roce 1994 byl výrazně upraven). Jedná se o**known-plaintext attack**, který je založený na nejednotné distribuci párů sousedních S-boxů za pomoci nastřádaných empirických rozdělení ze vstupních dat a zašifrovaných dat. Část klíče (bity) lze zjistit z dostatečného množství známých vstupních dat. Zbývající bity klíče lze následně zjistit z brute-force útoku.

V dnešní době se v některých případech využívá spíše 3DEX (triple-DES). Při zašifrování vstupních dat se data nejdříve zašifrují, poté dešifrují a následně znova zašifrují algoritmem DES. Velikost skupiny klíčů je 2^{112}.

3.1.3 Závěr

3.2 IDEA

3.2.1 Popis

International Data Encryption Algorithm (IDEA) je symetrická blokové šifra navržena v roce 1991 nahrazující existující šifru DES. Je postavena na šifře **Proposed Encryption Standard (PES)**. IDEA pracuje po 64bitových blocích za použití 128 bitového klíče. Celkový počet průchodů je 8,5 (8 identických transformací + vstupní transformace). Velká část bezpečnosti vyplývá ze střídání logických operací pracující s 16bitovými řetězci. Mezi použité operace se řadí modulární sčítání (2^{16}), modulární násobení ($2^{16}+1$) a bitová nonekvivalence XOR.

3.2.2 Prolomení

Již v roce 2011 proběhlo úspěšné prolomení IDEA s 8,5 průchody pomocí **meet-in-the-middle attack (MITM)**. Tento útok se zaměřuje na blokové šifry a dokáže exponenciálně zredukovat počet permutací brute force při dešifrování textu, který byl zašifrován více jak jedním klíčem. Při útoku se provádí brute force jak na vstupní data, tak i na zašifrovaný text blokové šifry. Následně se útočník snaží zašifrovat vstupní data s využitím klíčů za účelem vytvoření pomocného zašifrovaného textu (při šifrování byl použit pouze jeden klíč). Současně se útočník snaží dešifrovat zašifrovaný text pomocí různých klíčů na vstupní data, která budou totožná s daty, která byla využita

pro šifrování. Pokud se vstupní data shodují, je zde velká pravděpodobnost, že klíče použité při šifrování a dešifrování jsou dva klíče použité v blokové šifře. Podmínky pro tento útok jsou: vysoká kapacita disku pro uložení všech možností zašifrovaného textu a vstupních dat. Útočník má možnost pouze přistupovat k již vytvořeným datům, nelze si vytvářet nová. Proto se tento útok značí jako pasivní. Neplést si to s útokem **man in the middle**.

V roce 2012 byla IDEA znovu prolomena. Při lámání byl použit **narrow-bicliques attack** s redukovanou šifrovací sílou 2 bitů. Biclique útok je varianta útoku MITM. Šifra používá biclique strukturu (úplný biparitní graf, každý vstupní bod je propojen s každým výstupním bodem) k rozšíření počtu kol, které lze potencionálně napadnout.

3.2.3 Závěr

3.3 AES

3.3.1 Popis

Advanced Encryption Standard (AES), jinak nazývaná jako **Rijndael**, je symetrická bloková šifra. Při šifrování je použit blok dat o velikosti 128 bitů, zatímco klíč může být ve 3 velikostech: 128/192/256 bitů. Samotné šifrování probíhá ve 4 krocích po X iteracích (záleží na použité velikosti klíče, pro 128/192/256 bitů klíče je použito 10/12/14 iterací). Na samotném začátku šifrování jsou vstupní data zkombinována s podklíčem za pomoci operace XOR. Dále se pro N-1 iterací provádí následující postup:

1. **SubBytes (Záměna bytů)** – každý byte je nahrazen jiným bytem podle vyhledávací tabulky
2. **ShiftRows (Prohození řádků)** – každý řádek stavu je postupně posunut o určitý počet kroků
3. **MixColumns (Kombinace sloupců)** – zkombinování čtyř bytů v každém sloupci (nejnáročnější operace)
4. **AddRoundKey (Přidání podklíče)** – na celý blok dat je aplikován podklíč za pomoci operace XOR

V poslední iteraci se postup opakuje bez třetího kroku.

3.3.2 Prolomení

V dnešní době je šifra AES pro nejmenší použitelný klíč o velikosti 128 bitů stále neprolomená. Ani samotná NSA není schopna tuto šifru prolomit. Pro

prolomení plné AES šifry pomocí brute-force útoku by bylo potřeba uložit 2^{88} bitů dat (38 bilionů terabytů, což je více dat než bylo v roce 2016 uloženo na všech počítačích na planetě).

Mezi první známější útoky lze zmínit první **known-key distinguishing attack**, který dokázal dešifrovat zkrácený AES s 8 iteracemi. Při dešifrování byla časová náročnost 2^{48} a paměťová náročnost 2^{32}. Protože AES s klíčem o velikosti 128 bitů využívá 10 iterací, tak tento útok není efektivní.

Jako druhý útok lze zmínit **key-recovery attacks** v roce 2011 a lze ho nazvat i jako **biclique attack**. Nejlepší výsledky tohoto útoku při získávání klíče jsou: pro AES 128 bit klíč je potřeba 2^{126} operací, pro AES 192 bit klíč je potřeba $2^{189,9}$ operací a pro AES 256 bit klíč je potřeba $2^{254,3}$ operací.

3.3.3 Závěr

4 Asymetrické šifry

Asymetrické šifry využívají při šifrování dva odlišné klíče, veřejný a privátní. Veřejný klíč se používá pro zašifrování vstupních dat, zatímco privátní se využit pro dešifrování zašifrovaných dat. Hlavní výhoda těchto šifer spočívá v tom, že není nutné znát privátní klíč při šifrování a veřejný klíč při dešifrování (eliminace výměny klíčů). Bezpečná asymetrická šifra je taková šifra, která při šifrování používá dostatečně složité matematické problémy (prvočíselný rozklad násobku dvou velkých prvočísel nebo počítání diskrétního logaritmu). Do této dokumentace jsem vypsal 3 z nejznámějších asymetrických šifer(RSA, ElGamal, **??**).

4.1 RSA

4.1.1 Popis

Rivest-Shamir-Adleman (RSA) je jedna z prvních asymetrických šifer a používá se i v dnešní době pro šifrování i pro elektronické podepisování. Při zašifrování vstupních dat se vypočítává hodnota eulerovy funkce z 2 náhodných prvočíšel, ze které se následně vypočítává soukromý klíč. Veřejný klíč se volí náhodně za podmínky, že zvolená hodnota veřejného klíče je nesoudělná s vypočtenou hodnotou eulerovy funkce.

4.1.2 Prolomení

Při zjišťování klíče se používají dvě náhodně zvolená (nejlépe velká) prvočísla, je velice obtížné zjistit součin velkého čísla na dvě prvočísla (faktorizace).

Nelze v rozumném čase nalézt dva činitele, neboť není znám algoritmus faktorizace, který by pracoval v polynomiálním čase vůči velikosti binárního zápisu čísla N.

Za určitých podmínek ale lze rozlušit zprávu zašifrovanou algoritmem RSA. Mezi útoky lze uvést **Coppersmith' attack**. Tento útok popisuje skupinu útoků na veřejný klíč RSA šifrování, které jsou založeny na Coppersmithově metodě. Útoky jsou úspěšné za podmínek, že při šifrování je zvolen malý veřejný klíč nebo je k dispozici částečná znalost privátního klíče. Celkem lze uvést tři útoky založené na větách v Coppersmithově metodě:

1. **2. věta – Håstad: Håstad's broadcast attack**
2. **3. věta – Franklin-Reiter: Franklin-Reiter related-message attack**
3. **4. věta – Coppersmith: Coppersmith's short-pad attack**

4.2 ElGamal

4.2.1 Popis

ElGamalovo schéma je asymetrická šifra pro šifrování klíčů, které se využívají u symetrických šifer. Je založena na **Diffie-Helmanovo** výměně klíčů. ElGamal poskytuje další vrstvu zabezpeční asymetrickým šifrováním klíčů používaných dříve pro symetrické šifrování zpráv.

4.2.2 Prolomení

Při prolamování ElGamalova schématu je potřeba vyřešit problém diskrétního logaritmu.

Jeden z nejznámějších algoritmů, pomocí kterého lze zjistit privátní klíč použití u šifer stavěných na ElGamalovo schématu (například DSA), je algoritmus **Pollard's rho algorithm**. Tento algoritmus se zaměřuje na rozklad prvočísel. Algoritmus používá pouze malé množství datového prostoru a očekávaný běh času je úměrný odmocninou velikosti nejměnšího faktoriálu složeného čísla, který je rozkládán.

4.2.3 Závěr

5 WiFi šifry

5.1 WEP

5.1.1 Popis

5.1.2 Prolomení

5.1.3 Závěr

5.2 WPA1/WPA2

5.2.1 Popis

5.2.2 Prolomení

5.2.3 Závěr

6 Závěr