Západočeská univerzita v Plzni

Bezpečnost v informačních technologiích

KIV/BIT

Dokumentace semestrální práce

Vojtěch Daniš́ík
A16B0019P
danisik@students.zcu.cz

15. května 2019

Obsah

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 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. Bezpečnost každého šifrovacího systému závisí na dvou věcech: "matematické bezpečnosti"a "implementační bezpečnosti".

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 bloková 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.

- **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 výstupů 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 3DES (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

V dnešní době se využívání DES silně nedoporučuje, protože rozšifrování pomocí brute-force útoku lze zvládnout za méně než 24 hodin, kdy brute-force útok je jeden z nejvíce časově náročných útoků.

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. Útok probíhá tak, že se pokoušíme zašifrovat vstupní text pomocí zvoleného šifrovacího algoritmu s využití seznamu klíčů, které jsou zjištěny ještě před samotným začátkem pomocí brute-force. Po zašifrování vstupního textu a uložení kombinací klíče a zašifrovaného textu do tabulky je tento postup opakován ale s tím rozdílem, že vstupní text se pokoušíme dešifrovat s využitím seznamu

klíčů. Následně se porovnávají hodnoty vytvořených tabulek. Pokud byl nalezeny dva stejné záznamy v tabulkách, jsou klíče těchto záznamů uloženy do nové tabulky T. Na samotném konci jsou uložené páry v tabulce T otestovány stejným způsobem a kontroluje se jejich validita. V případě, že tento pár klíčů nefunguje na pár vstupních dat, je tento pár vstupních dat znovu otestován pomocí MITM. 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 založen na meet-in-the middle útoku. Tento útok lze aplikovat jak na blokové šifry, tak i hashové funkce. Šifra používá biclique strukturu (úplný biparitní graf, každý vstupní bod je propojen s každým výstupním bodem) k rozšíření počtu kol, které lze potencionálně napadnout. V praktickém hledisku je tento útok proti šifře IDEA neškodný, protože výpočetní složitost je rovna $2^{126.1}$.

3.2.3 Závěr

Šifra IDEA je i přes dva úspěšné útoky stále bezpečná pro praktické účely, protože pro oba dva útoky vedené proti IDEA je potřeba velké množství datové kapacity a jsou vysoce časově náročné.

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).

Jako první útok lze zmínit **eXtended Sparse Linearization attack (XSL)**. Tento útok na svém začátku analyzuje interní strukturu šifry a z toho následně odvodí systém kvadratických souběžných rovnic. Tyto systémy rovnic jsou ve výsledku velmi velké (například 8000 rovnic s 1600 proměnými pro 128-bitový AES). Pro vypočítání těchto rovnic je využit algoritmus XSL (eXtended Sparse Linearization), pomocí kterého lze zjistit klíč. XSL algoritmus lze provést ve třech způsobech. První způsob zahrnuje vyřazení těch rovnic, které obsahují subklíče blokové šifry (je potřeba velké množství párů vstupní text-zašifrovaný text). Druhý způsob naopak využívá rovnice, které obsahují subklíče (pro fungování stačí jeden pár vstupního textu-zašifrovaného textu). Třetí způsob, neboli compact XSL, rozšiřuje systém kvadratických rovnic jejím vynásobením vybranými monomiály určitého stupně (monomiál je pojem polynomu).

Jako druhý útok lze zmínit **key-recovery attacks** (mezi tyto útoky lze zařadit i brute-force) v roce 2011 . 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. Jednalo se pouze o teoretické útoky, nikoli praktické.

3.3.3 Závěr

AES šifra je stále nikým neprolomená a proto ji lze označit za vhodnou při šifrování dat.

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 jednu z nejznámějších asymetrických šifer(RSA).

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.

- Lze zmínit útok **DROWN (Decrypting RSA with Obsolete and Weakened eNcryption)**, který byl veden na protokoly TSL podporující nezabezpečené SSLv2 protokoly. DROWN využívá **Adaptive chosen-ciphertext attack** s použitím SSLv2 protokolu. Pro dosažení tohoto útoku je potřeba mít velice velký výpočetní výkon. OpenSSL protokol měl v době nálezu DROWN útoku větší problém, protože se na tento protokol dal aplikovat speciální DROWN útok, který z důvodu drastického snížení nutnosti výpočetního výkonu umožňoval provést **man-in-the-middle 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

- **Chosen-ciphertext attack** – Tento útok ja založen na vybrání množiny šifrovaných dat, které jsou následně dešifrovány.
- **Adaptive chosen-ciphertext attack** – Rozdíl oproti neadaptivnímu chosen-ciphertext útoku je ve vybírání množiny šifrovaných dat. Na samém začátku je vybrána podskupina šifrovaných dat, která jsou následně dešifrována. Na základě výsledku z prvního dešifrování je vybrána druhá podskupina šifrovaných dat, která je následně také dešifrována. Tento postup se opakuje až do konce množiny šifrovaných dat.
- **Man-in-the-middle attack** – Princip útoku spočívá v odposlouchávání komunikace mezi účastníky tak, že útočník se stane aktivním prostředníkem. Viz aféra Superfish s firmou Lenovo, kdy firma Superfish instalovala vlastní kořenový certifikát do nových počítačů firmy Lenovo, který analyzoval veškerý HTTPS provoz ve webovém prohlížeči a pomocí injektování JavaScriptového kódu do navštěvovaných webových stránek vkládal reklamy na základě historie prohlížení důvěřivého uživatele.

4.1.3 Závěr

V dnešní době je RSA šifra při použití dostatečně velkého klíče neprůlomná a je doporučeno ji používat jak pro šifrování, tak i pro elektronický podpis za případu, že při komunikaci není použit protokol SSLv2, který v dnešní době není podporován.

5 Zajímavost - eyeDisk

eyeDisk je nově vytvořené USB flash zařízení, které v sobě obsahuje zařízení Iris pro rozpoznávání duhovky uživatele, které se používá pro odemykání USB (firma vyvinula vlastní rozpoznávací algoritmus, který není do této doby zveřejněn). Data jsou zašifrována 256-bitovým AES algoritmem, podporuje USB verze 3.0 a je kompatibilní jak s Windows, tak i Mac OS. Startovní cena pro 32GB verzi je necelých 60$.

O této flashce se říká, že má být neprůlomná, a proto se strhlo šílenství o to, zda ji dokáže někdo prolomit a získat data uložená na zmíněném USB disku. Jako prvnímu se to povedlo Davidu Lodge-mu, který dokázal prolomit zabezpečení. Podařilo se mu to díky zveřejnění hesla v nezašifrované podobě při záložním přihlašování. Při záložním přihlašování si uživatel

nejdříve nastaví heslo v případě, že selže zařízení/technologie skenování duhovky. Přihlašování u této flashky probíhá tak, že se aktuálně zadané heslo porovná se záložním heslem, které se nachází v paměti zařízení a lze ho zachytit při komunikaci a to i v případě zadání neplatného hesla. Při komunikaci dokonce objevil i hash své duhovky.

6 Závěr

V dokumentu byly vybrány celkově 4 šifry, na kterých jsem popsal množství možných útoků, které dokáží některé šifry prolomit jak teoreticky, tak i prakticky. V praktickém případě lze prolomit hlavně šifru DES a za určitých podmínek (v dnešní době nemožné) i šifru IDEA. Naopak šifra AES se zdá být stále neprolomitelná z důvodu velkého množství iterací při šifrování a velikosti použitých klíčů. Mezi neprolomitelné šifry lze zařadit i šifru RSA za podmínky, že server nebude nikdy šifrovat komunikaci se vzdálenými servery pomocí protokolu SSLv2.