SMS007 – ochrana Vašich dat vědeckými metodami

Tento text je určen pro ty uživatele systému SMS007, kteří se chtějí dozvědět něco více o způsobu, jímž systém SMS007 chrání jejich data před odposlechem či pozměněním.
Jsou zde popsány základní metody současné ochrany dat, a rovněž způsob, jakým systém SMS007 těchto metod využívá k zabezpečení Vaší komunikace.

1. Moderní kryptografie – ochrana soukromí pro každého

V dřívějších dobách byla ochrana dat doménou vojska či policie. Ještě v 50. letech 20. století se téměř veškerý vědecký výzkum v oblasti ochrany dat odehrával za zdmi střežených státních institucí.

Zásadní změnu přinesla až 70. léta, kdy počítače začaly v čím větší míře pronikat do civilního světa. Cenná data byla ukládána na pevné disky a posílána na druhou stranu světa skrz počítačové sítě. Problém neoprávněného přístupu k nim se rychle stal velmi palčivým. Průmyslová špionáž, sledování provozu na síti, kopírování citlivých dat bez souhlasu majitele – to vše ohrožovalo osobní bezpečnost a majetek milionů lidí a tisíců obchodních společností. Takřka „přes noc“ vznikla všeobecná poptávka po kvalitní ochraně dat přístupné civilnímu sektoru.

Tato poptávka našla svoji odezvu v prudkém rozvoji vědecké kryptografie – odvětví, které leží na pomezí matematiky a informatiky. Množství vědců pracujících v oblasti kryptografie vzrostlo brzy několikanásobně. Jejich základním úkolem bylo objevit co nejspolehlivější postupy – algoritmy – které by uživatelé počítačů mohli nasadit ke kvalitní ochraně svých dat.

2. Symetrické šifrování

Typickým způsobem, jak dnes chránit data, je nasazení tzv. symetrické šifry. Způsob použití takové šifry je velmi jednoduchý. Jediné, co obě strany potřebují, je společný *klíč* a stejnou šifru (algoritmus). Společný *klíč* musí být držen v tajnosti oběma stranami. Může jím být například společně dohodnuté heslo.

Odesílatel: klíč + šifra + původní zpráva ----------> zašifrovaná zpráva.

Zašifrovaná zpráva je změtí nesmyslných znaků, ze které není bez znalosti klíče možno zjistit, co obsahuje. Může být odeslána příjemci např. internetem nebo přes SMS, aniž by hrozilo riziko jejího odposlechu – i když ji někdo zachytí, nic se z ní nedozví.

```
ThAEhrKKINUxToL9T+SslI9ROvFfYXNBT87wxpgqAElaQv/sDDajHO/ZV0IrOZAW
kJV3xQ2csQ8qX2IhMUO9gq/R7FlyvbmJkpJKtDHSIRtrMDxw5LPpU41eqeZjc3ED
```

Příklad zašifrované zprávy

Příjemce: klíč + šifra + zašifrovaná zpráva ----------> původní zpráva.

„Symetrická šifra“ je podobně obecný pojem jako „auto“. Stejně jako existuje mnoho druhů aut, existuje i mnoho druhů symetrických šifer. Tyto šifry se navzájem liší svojí kvalitou. Některé šifry se postupem času ukázaly být špatně navržené (např. FEAL), některé technicky zastaraly (například DES). Nejlepší skupinou šifer jsou ty, které jsou známy mnoho let, a přesto odolaly všem pokusům vědců o zlomení. Jejich zástupci jsou například AES, Blowfish či IDEA.

3. Kerckhoffův princip

S ochranou dat souvisí tzv. Kerckhoffův princip, poprvé vyslovený pruským důstojníkem Kerckhoffem již před 150 lety.

Utajení a bezpečnost zašifrovaných dat nesmí záležet na utajení postupu, kterým se šifrují. Naopak, vždy se musí předpokládat, že váš nepřítel zná šifru (algoritmus) do nejmenších detailů. Utajení musí spočívat pouze v klíči (např. hesle), které nezná nikdo jiný.

Tento princip je dnes všeobecně uznáván jako základ úspěšné ochrany dat. Proto se vědci soustředili na vytvoření co nejlepších, veřejně známých šifrovacích postupů (algoritmů), a na ověření toho, že tyto postupy jsou bezpečné.

Takovými postupy jsou například symetrická šifra AES či hashovací funkce SHA-2. Jejich bezpečnost je ověřena tím, že i přes mnohaletou práci mnoha tisíc vědců se nikomu z nich nepodařilo objevit způsob, jak tyto postupy „rozbít“.

Skutečně kvalitní systém pro ochranu dat je takový systém, jehož vnitřní funkčnost a detaily jsou dobře známy, ale přesto tato znalost ani v nejmenším nepomůže potenciálním protivníkům v jejich zlomení. Příkladem takového systému je například veřejně popsaný protokol TLS. S jeho pomocí jsou chráněny například bankovní operace při Internet bankingu, tedy transakce velké hodnoty.

4. Symetrická šifra AES

AES (Advanced Encryption Standard) je šifrovací postup, který je v současnosti používán pro ochranu nejcitlivějších informací. Vznikl v roce 1998, když byla vypsána mezinárodní soutěž o kvalitní šifrovací algoritmus, který by nahradil do té doby používaný standard DES (Data Encryption Standard) z roku 1976. Zemí jeho původu je Belgie.

Symetrická šifra AES si už v průběhu mezinárodní soutěže vysloužila velkou pozornost vědecké komunity, neboť je velmi rychlá, a přesto velmi bezpečná. Přes mnohaleté úsilí se nezdařilo najít v šifře AES žádnou slabinu. Z tohoto důvodu je dnes AES používána k ochraně velkého množství citlivých dat v civilním i vojenském sektoru. Na šifru AES spoléhá například americká diplomacie a armáda.

Standard AES připouští klíče délek 128, 192 a 256 bitů. Nejvyšší délka klíče – 256 bitů – byla americkou NSA (National Security Agency) doporučena k ochraně dat klasifikovaných jako „přísně tajné“.

5. Hashovací funkce SHA-2

SHA-2 je standardem, s jehož pomocí mohou být data chráněna před pozměněním. SHA-2 odvodí z každého textu jeho „otisk“ (fingerprint). I sebenepatrnější následná změna v textu se pak projeví naprostou změnou jeho „otisku“: tak je možno zjistit, že do textu někdo zasáhl. SHA-2 se využívá v případech, kdy je zapotřebí zajistit, aby text zprávy nebyl „po cestě“ protivníkem pozměněn. Taková situace nastává například u digitálních podpisů.

6. SMS007 – moderní kryptografie ve Vašich službách

Systém SMS007 využívá k ochraně Vašich dat všech výše zmíněných výdobytků moderní kryptografie. Jeho návrh se drží Kerckhoffova principu, podle nějž znalost samotného postupu nesmí ohrozit bezpečnost systému. Proto Vám zde můžeme popsat samotný způsob šifrování.

6.1 Hlavní heslo aplikace

Základem Vaší bezpečnosti je „hlavní heslo“, které si zvolíte při prvním startu. Je to jediné heslo, které si musíte pamatovat pro práci se systémem. Systém SMS007 vyžaduje, aby toto heslo bylo dlouhé minimálně 8 znaků.

Na kvalitní volbě tohoto hesla záleží Vaše bezpečnost. Jestliže si zvolíte snadno uhodnutelné heslo (například běžné slovo, nebo datum narozenin), Váš protivník by se mohl pokusit toto heslo uhodnout. V případě, že toto „hádání“ bude prováděno počítačem, může být snadno vyzkoušeno několik milionů slov. Volte tedy heslo tak, aby obsahovalo zároveň velká a malá písmena, a rovněž číslice.

Jelikož „hlavní heslo“ budete používat při každém startu systému, nehrozí přílišné nebezpečí, že byste jej zapomněli. Pokud jej však zapomenete, Vaše zašifrovaná data jsou navždy ztracena! Bez znalosti „hlavního hesla“ neexistuje žádný postup, jakým by bylo možno je přečíst.

Z „hlavního hesla“ je pomocí funkce SHA-2 odvozen klíč, který se použije pro zašifrování všech dat ukládaných do telefonu (např. přijaté zprávy či seznamy kontaktů). K tomuto šifrování se používá již zmíněná šifra AES, běžící v tzv. CBC-módu.

6.2 Praktické použití hlavního hesla

V okamžiku, kdy aplikace startuje, dotáže se Vás na „hlavní heslo“. Jakmile zadáte do políčka pro heslo nějaký text a stisknete OK, převede aplikace tento text pomocí funkce SHA-2 na klíč a s tímto klíčem se pokusí rozšifrovat data uložená šifrovaně v telefonu. Pokud se jí to podaří, šlo o správné heslo. Pokud se jí to nepodaří, bylo heslo zadáno špatně, a Vy budete varován, že není možno pokračovat dále.

6.3 Změna hlavního hesla

V případě, že usoudíte, že si přejete svoje hlavní heslo změnit, můžete tak učinit v nabídce Nastavení aplikace. Ke změně hesla je zapotřebí jednou zadat heslo staré a dvakrát heslo nové (abyste neudělali neúmyslný překlep), a stisknout OK. Všechna data uložená v telefonu se přešifrují pomocí nového hesla, a od té chvíle musíte používat heslo nové.

6.4 Šifrování SMS zpráv

K tomu, aby si dva lidé vlastnící systém SMS007 mohli psát šifrované zprávy, musejí si nejprve domluvit další společné heslo, které nesmějí nikomu dalšímu prozradit. Toto heslo se ukládá do telefonu, kde je bezpečně chráněno před přečtením nepovolanou osobou tím, že je zašifrováno pomocí „hlavního hesla“ aplikace.

Čím složitější a komplikovanější společné heslo si dva lidé dohodnou, tím lépe. Jelikož společné heslo si uloží jen jednou, a pak si jej už nemusejí pamatovat, může být opravdu *velmi* dlouhé a komplikované. Vhodným způsobem, jak vytvářet dlouhá a komplikovaná hesla, je například vzít nějakou větu, a použít první písmena všech slov. **N**apříklad **t**ato **v**ěta **b**y **t**akto **v**ytvořila **n**ásledující **h**eslo:

Ntvbtvnh

Počet možných vět v jakémkoliv lidském jazyce je astronomický, takže tímto způsobem se dají vytvářet poměrně bezpečná hesla. Nejlepší je ovšem používat hesla zcela náhodná. Detaily najdete v manuálu, v sekci „Doporučená délka hesel“.

Zpráva SMS, kterou chce jeden člověk odeslat druhému, je zašifrována standardem AES za pomoci klíče odvozeného pomocí funkce SHA-2 ze společného hesla.

6.5 Detaily použitých postupů

V případě, že má být text T zašifrován pomocí klíče K, postupuje systém SMS007 následovně:

i. Nejprve zjistí, jaký je aktuální čas C. Následně spočítá SHA-2 z textu T a času C. Tento kód, označíme jej H, bude sloužit k ochraně zprávy před pozměněním.
ii. Umístí do jednoho bloku ochranný kód H, čas C, několik dalších drobných informací (např. délku textu) a text T.
iii. Výsledný blok zašifruje pomocí klíče K šifrou AES v módu CBC (Cipher Block Chaining). Vznikne zašifrovaný text Z, který se může bezpečně uložit či odeslat.

Přítomnost kódu H v zašifrovaném textu zajišťuje ochranu tohoto textu před pozměněním „zvenčí“. Skutečnost, že kód H se počítá nejen z textu T, ale i z času C, zajišťuje, že dokonce i tentýž text T zašifrovaný tímtéž klíčem K dá při dvou různých příležitostech vzniknout dvěma různým zašifrovaným textům Z_1 a Z_2.

6.6 Bezpečnost, heslo a klíče

AES je velmi bezpečná šifra, při níž ani znalost zároveň textu T a zašifrovaného textu Z nepomůže protivníkovi odhalit klíč K. Je však velmi důležité volit kvalitní klíč K (respektive heslo, z nějž je odvozen). Jelikož „společné heslo“ pro komunikaci si lidé nemusejí pamatovat, silně doporučujeme, aby bylo voleno co nejdelší, nejkomplikovanější a nejpodivnější. Protivník se pravděpodobně bude snažit vyzkoušet co nejvíce běžných českých slov. Je zapotřebí nedat mu v tomto směru šanci.
Nezapomeňte: bezpečnost Vaší komunikace záleží na kvalitě „společných hesel“, která si se svými partnery domluvíte!