Fakulta informatiky

MASARYKOVA UNIVERZITA
PS 2013

January 6, 2014

Zkouška z předmětu PV079 – Applied Cryptography

Deadline 8:09, 7. 1. 2014. Řešení je nutno odevzdat ve složce „Solutions to the exam, Jan 6–7" v odevzdávárně předmětu v ISu. V případě elektronické formy odevzdání je plně na odpovědnosti studenta, jestli bude odevzdané zadání čitelné. Akceptované formáty jsou PDF čitelný Adobe Acrobat Reader 11.0.5, Microsoft Word čitelný verzí 2010, nebo dokument čitelný OpenOffice 3.4.1 Writer.

Pište, prosím, čitelně a každý list odpovědi očíslujte a označte jménem. Odpovědi by měly být stručné, ale úplné. *Vzájemná spolupráce se nepovoluje!!!*

0. Dešifrování (10 bodů):

Za 1. světové války jste našli na německé frontě následující tabulku. Má šest sloupců i řádků a jejich záhlaví byla vždy se stejnými písmeny – A, D, F, G, V a X. Ale pořadí prvků v tabulce bývají vždy různá – ovšem vždy má 26 písmen a 10 číslic.

	A	D	F	G	V	X
A	K	Z	W	R	1	F
D	9	B	6	C	L	5
F	Q	7	J	P	G	X
G	E	V	Y	3	A	N
V	8	O	D	H	0	2
X	U	4	I	S	T	M

Pak jste našli proužek papíru se třemi řádky:

Zpráva: ..... zbytek tohoto řádku byl bohužel zaretušován ...,
Mezi: AF XF DV VG ..... GA AG
Šifra: VXVA AGXG FGFX VXVR DVXA FDGG XAXF
G

Pak jste našli tabulku, ve které byla záhlaví sloupců v předcházejících případech různá, ale vždy byla označena různými písmeny z 26-znakové abecedy.

D	E	U	T	S	C	H
A	F	X	F	D	V	V
G	G	A	D	V	X	X
X	F	X	G	X	V	V
G	X	F	G	A	A	G

1. Prostudujte tyto materiály a určete systém zašifrování a dešifrování a také, samozřejmě, původní text zprávy.

2. Způsobuje zašifrování nárůst délky zprávy? Jestliže ano, pak určete faktor tohoto nárůstu.

3. Jedná se o substituci, transpozici nebo kombinovanou šifru?

4. Jaká je délka klíče? Jaká je „délka bloku" algoritmu?

5. Jedná se o slabou nebo kvalitní šifru? Proč?

1. Kabelová televize (10 bodů): Místní společnost Kabelovka Minus zavedla systém, kdy uživatel platí pouze za vybrané filmy. Signál je veden do bytu, kde speciální zařízení provede některé úpravy (signálu) a poté jej předá TV přijímači. Toto zařízení je pevně spojeno s přijímačem. Ovšem studenti místní průmyslovky nalezli způsob jak zařízení nahradit podomácku vyráběným obvodem.

K příjmu filmu je tedy vydáván klíč K_i při zavedení služby, kdy je klíč naprogramován do paměti zařízení a jeho kopie je také uložena v bezpečné databázi společnosti. Každý film F se skládá z několika GB dat a je kabelem doručen do každé domácnosti. Uživatelova žádost o shlédnutí filmu je autentizována nějakými daty odvozenými z K_i a zvláštní relační klíč pro určitý film je pak uživateli dodán do zařízení u TV před zahájením vysílání filmu. Zvažte (a popište) výhody a nevýhody následujících metod (bezpečnost, náročnost realizace ze systémového hlediska, cena implementace/provozu atd.)

- Film F je šifrován klíčem K_i pro každého uživatele U_i, kterému je posílán proud bitů $E_{K_i}(F)$.
- Systém Kabelovky Minus vytvoří speciální klíč K_{FX} pro každý film F a před začátkem filmu pošle každému (film požadujícímu) uživateli U_i hodnotu $E_{K_i}(K_{FX})$. Zařízení u TV uživatele pak obnoví K_{FX}. Kabelem je vysílána jediná kopie filmu – $E_{K_{FX}}(F)$.
- Schéma z předcházejícího případu je modifikováno tak, že uživateli U_i je posílán klíč K_{FX} jako $K_{FX} \oplus K_i$, aby se ušetřily náročné operace šifrování.

2. Mobilní telefon (10 bodů) – mobilní telefonní systém se (pro naši zjednodušenou představu) skládá z uživatelského přístroje, stanic jednotlivých buněk/základen a datové komunikační sítě mezi buňkami o dostatečné kapacitě. Při telefonování jsou data přenášena rádiovým spojením z přístroje na stanici buňky a odtud se dostávají na datovou komunikační síť, popř. běžnou telefonní sít. Po síti jsou směrována na další určenou stanici buňky a z té přenášena rádiovým spojením na přístroj druhého komunikujícího uživatele.

Pro zajištění správného účtování poplatku je potřeba provést autentizaci uživatelského přístroje. Autentizační protokol využívá veřejně dostupný generátor pseudonáhodných čísel RANDY, který je implementován ve všech prístrojích i stanicích všech buněk. Pseudonáhodné číslo x se generuje – $x = RANDY(t)$ – z počáteční hodnoty t. Každý přístroj P_i obsahuje unikátní tajný symetrický klíč K_i, který je také stanicím dostupný prostřednictvím komunikační sítě.

Autentizace spočívá v zaslání výzvy v podobě náhodného čísla r ze stanice do přístroje a poté v zaslání odpovědi o z přístroje do stanice. Stanice srovná o s hodnotou, kterou očekává (neboť zná algoritmus výpočtu i vstupní parametry). V případě správné odpovědi umožní uživateli navázat hovor, příp. ustavit tajný klíč relace, také účtuje poplatky uživateli U_i.

Zamyslete se a popište vhodnost následujících schémat. Předpokládejte, že jakýkoliv útočník má možnost odposlouchávat všechny rádiové hovory, je schopen vysílat vlastní zprávy na dané frekvenci a uchovávat všechny již vyslané zprávy pro případnou analýzu. Přístroj uživatele je konstruován tak, že automaticky odpovídá na každou výzvu r, kterou obdrží rádiovým spojením (se svým veřejně známým identifikačním číslem).

- r je náhodné číslo a
  $o = RANDY(K_i) \oplus r$;
- r je sekvenční číslo (počitadlo) udržované stanicí a zvětšované o 1 vždy, když stanice vyzývá P_i
  $o = RANDY(K_i \oplus r)$;
- r je náhodné číslo a
  $o = RANDY(K_i \oplus r)$.

3. Kryptografická ochrana hesel (10 bodů): LidoBanka se rozhodla provozovat služby telefonického bankovnictví v Indii a datové centrum umístila v Rumunsku. Pro autentizaci klientů telefonického bankovnictví se používá následující schéma: Klient dříve určil své tajné heslo, které se skládá z minimálně osmi alfanumerických znaků, např. AUTEN007TIZACE. Pro povolení aktivních operací telefonického bankovnictví je operátorovi určena systémem náhodná dvojice pozic znaků v hesle - operátor z Indie pak vyzve klienta k udání znaků na těchto dvou pozicích. Např. pro pozice 2 a 8 musí klient sdělit U a 7. Pokud klient nesdělí oba znaky správně, pak nejsou ani operátorovi umožněny operace v systému jménem klienta. Operátorovi také nejsou zobrazeny žádné znaky hesla - jen pozice a následně informace, zda oba znaky byly klientem sděleny správně (při nesprávném zadání jednoho znaku není ani operátorovi sděleno to, který znak byl zadán správně a který nesprávně). Při nesprávném zadání požadované dvojice znaků je určena nová náhodná dvojice pozic znaků v hesle, které operátor požaduje. Při třech po sobě následujících nesprávných zadáních dvojic znaků je dále manipulace s účtem zablokována a následují další postupy, které nás v tomto úkolu nezajímají.

Zvažte možnosti zajištění ochrany základními kryptografickými mechanizmy - jak hesel uložených v Rumunsku, tak kandidátských dvojic zadaných operátorem podle instrukcí klienta při přenosu z Indie do Rumunska. Stanovte přesně použité kryptografické algoritmy a jejich módy činnosti. Nesmíte spoléhat na žádný tunelovací/VPN protokol, jako např. TLS nebo IPv6.

Navrhněte alespoň dvě odlišné metody. Zvažte (a popište) výhody a nevýhody těchto metod - minimálně s ohledem na bezpečnost, náročnost realizace ze systémového hlediska, cenu implementace a provozu, rychlost.

4. Bezpečnostní bankovní API (10 bodů): V jedné zahraniční bance vyšlo manažerské nařízení, že veškeré uživatelské PINy budou povinně šestimístné, a že banka nově navíc začne podporovat až patnáctimístná čísla účtů. Tato změna měla dopad na drtivou většinu systémů využívajících pro bezpečnou práci s PINy právě hardwarové bezpečnostní moduly (HSM). Aby bylo možné s šestimístnými PINy a s patnáctimístnými čísly účtu v HSM bezpečně pracovat, bylo zavedeno následující rozšíření stávajícího aplikačního programovacího rozhraní (API).

Pro formátování PINu do 64bitového bloku CPB byl zaveden nový mód formátování PINů – ANSI X9.8six. Oproti původnímu módu ANSI X9.8 měl blok P1 zafixovánu délku PINů právě na 6 a s výjimkou první pozice navíc umožňoval plně využít celý 64bitový blok P2, čímž bylo dosaženo podpory pro až patnáctimístná čísla účtů ($P_2 = 0aaaaaaaaaaaaaaa$, kde a je číslice čísla účtu).

Popište dopady těchto změn na původní ANXI X9.8 útok a na útoky pomocí tzv. decimalizační tabulky.

1. Spočítejte, jak lze pomocí útoku ANSI X9.8, útoku pomocí decimalizační tabulky bez využití offsetů, a útoku pomocí decimalizační tabulky s využitím offsetů obecně redukovat prostor uživatelských PINů (uveďte nejlepší i nejhorší případ). Nezapomeňte, že některé číslice se v PINu mohou opakovat.

2. Spočítejte, kolik volání funkcí API budete potřebovat v útoku ANSI X9.8, v útoku s pomocí decimalizační tabulky bez využití offsetů, a v útoku pomocí decimalizační tabulky s využitím offsetů. I zde nezapomeňte, že některé číslice se v PINu mohou opakovat.

3. V případě útoku pomocí decimalizační tabulky s i bez využití offsetů" dále rozepište, jaké jsou složitosti útoků (redukce prostoru PINů a počty volání funkcí API) pro následující PINy: PIN1=112233, PIN2=122334 a PIN3=123455.

Vašek Matyáš