Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego

Laboratorium z przedmiotu: Wprowadzenie do Kryptologii

Sprawozdanie z ćwiczenia laboratoryjnego nr 3:

Funkcje skrótu

Prowadzący: mgr inż. Marta Turowska

Wykonał: Radosław Relidzyński

Grupa: WCY20IY4S1

Data laboratoriów: 11.05.2021 r.

Spis treści

A.	Treść zadania	2
В.	Użyte komendy	2
C.	Szyfrowanie pliku	2
	Użyte polecenia:	2
	Zawartość pliku "first_ecb.txt"	3
	Zawartość pliku "first_cbc.txt"	3
D.	Szyfrowanie pliku ze zmienionym bitem	
	Użyte polecenia:	4
	Zawartość pliku "second _ecb.txt"	4
	Zawartość pliku "second _cbc.txt"	
E.	Podsumowanie	

A. Treść zadania

Przy pomocy openssi wykorzystując szyfr AES zaszyfrować w trybie ECB plik, a następnie zaszyfrować w trybie CBC. Następnie zmienić 1 bajt w pliku i ponownie zaszyfrować szyfrem AES w trybie ECB oraz CBC. Porównać otrzymane wyniki i wyciągnąć wnioski. Podać możliwe zastosowania dla tych szyfrowań i ocenić bezpieczeństwo obydwu. Jako klucz użyć swój numer indeksu.

B. Użyte komendy

W programie openssl.exe wykonuję poniższe komendy:

```
aes-256-ecp, aes-256-cbc
```

Jako argument będę podawał plik wejściowy

```
-in {file_with_path}
```

Jako kolejne argumenty będę podawał ścieżkę do pliku wyjściowego

```
-out {file_with_path}
```

Jako klucz szyfrowania podam swój numer indeksu, czyli

76836

Aby móc dobrze porównać rezultat, dodam specjalną flagę

-nosalt

Następnie będę analizować pliki tekstowe zawierające zaszyfrowane wiadomości

Wywołanie odpowiednich poleceń

```
■ D\Program Files\Git\usr\bin\openssteve

OpenSSL> aes-256-ecb -nosalt -in D:\STUDIA\logo.bmp -out D:\STUDIA\first_ecb.txt
enter aes-256-ecb encryption password:
verifying - enter aes-256-ecb encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
OpenSSL> aes-256-cbc -nosalt -in D:\STUDIA\logo.bmp -out D:\STUDIA\first_cbc.txt
enter aes-256-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
OpenSSL> aes-256-ecb -nosalt -in D:\STUDIA\logo2.bmp -out D:\STUDIA\second_ecb.txt
enter aes-256-ecb encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
OpenSSL> aes-256-cbc -nosalt -in D:\STUDIA\logo2.bmp -out D:\STUDIA\second_cbc.txt
enter aes-256-cbc encryption password:
**** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
OpenSSL>
```

C. Szyfrowanie pliku

Użyte polecenia:

aes-256-ecb -nosalt -in D:\STUDIA\logo.bmp -out D:\STUDIA\first_ecb.txt aes-256-cbc -nosalt -in D:\STUDIA\logo.bmp -out D:\STUDIA\first_cbc.txt

Zawartość pliku "first ecb.txt"

first_ecb.txt — Notatnik

Plik Edycja Format Widok Pomoc 錞频№喺嵌铥極8萌80№N量拭懓□膽禐®稅8蝬÷∹姕88數ἀ蚨№徻敫鿏峭喙菓鏙艒噑88€│랖8️雙枴朮⊧與ध8債匙哭剝宿墣♡暑翺晖鲡暑劍シッ剎碧媽^ 回燒回艤買鈙槐鬛紳뮟:前╒眾暑衣兴乨敽犪悿燯€觋膈靺鮡╱楮趏Θ皎娉挫刭圆圆逶溫圆剺ы、圆Ծ細嵢藁盖剛廛Ф衞쯲┗圆ӛ鑌裎芰簪裔页暑湲軆‼闆샤賏焖 敖昊# 芳丹金属假確AD⊫B读ĀL學楊姷튁智图韓最照姚谝 ρ菔图邦達他AMHKII曝uBA叉籬 塵縷令奕絈 驅為亞縛 L镎瞡薙獸DID烏te弯頭習DD函繼元無期渾点 ╕Ў∥組횉堣栚儮╕Ў∥組횉堣栚儮╕Ў∥組횉堣栚儮╕Ў∥組횉堣栚儮╕Ў∥組횉堣栚儮╕Ў∥組輕堣栚儮╕Ў∥組횉堣栚儮╕Ў∥組暫堣栚儮╕Ў∥組離堣栚儮╕Ў∥組暫堣栚儮╕Ў∥組暫堣栚儮 雄欢줃귨딃芥澖団팼랔뚬嬬*/C註□冒造州燮點悁좲-安洋团團呈亡飠閗騹羪풙剽団呈薩8㎜突禩叮遇缉薪籲团囮虠最쁴嗧償闆蹈讀"矢돍む馭鮁♡焘剿媱ħ好剴┦먈瘡 병ጵና학례转懶隆픲찞뿠鮻마춌-매俜찞顚踻憴禠綨委吘괔酺袦찞奴黍冤羸ᠬ팽ು띠津驌額᠙ᡂ│仟찞⊷띶윘擿飽☜껝拧礋呍彪졍崀丁잣떼纯縋巶揰屛ശ뺘ኤ∭ ╕У∥組譽揭栚儮╕У∥組譽堣栚儮╕У∥組譽堣栚儮╕У∥組譽堣栚儮╕У∥組譽堣栚儮╕Ў∥組譽堣栚儮╕Ў∥組譽堣栚儮╕Ў∥組譽堣栚儮╕Ў∥組譽堣栚儮╕Ў∥組譽堣栚儮╕Ў∥組譽堣栚儮 屬岳絫鵥芏蜆撩回☞晌▲图△哖讠共荻友®踅每图抗彰州佐藤杭籐×邬堰榛绨牬Z鍢ۃ赛ᡂ觖α龝嫐齿欤랰嗕♀悑嚆Х鋐铕裎型图克暑篾嗍妗涚៙氊頣刈咒詈晃氝木 Ⅲ基残纖i酸B植浮羬ş寻珠募尋B₂BB奔遲滌录量較暾虹山PR三股这BB射≈響然®盆B毀腎褌₽荧t≡∞嬺眾E機影廢遡ゞB稅釋升ĜB蝴業區與鹽岸區 ╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮 坐釗⋾岦晧茬読誓٩シ『組횉堣栚儮٩シ『組횉堣栚儮٩シ『組횉堣栚儮٩シ『組횉堣栚儮٩シ『組횉堣栚儮٩シ『組횉堣栚儮٩シ『組暫堣栚儮٩シ『組暫堣栚儮٩シ『組暫堣栚儮٩シ『組暫堣栚儮٩シ『組暫堣栚儮9シ 奨会図∞ඎ讀Φ❷图響管望图→悟參巊綏图糾型闔: 圆燜庩镜~图镈樫昊橹序型股当閃鸷⊙洞A歌戳Y器✍兒虎c頤图香洌铷莜骴髛蚪楓氤┐睧%望仅阕,螳Ⅲ硍Ÿ禈癳圆釒 ╕Ў∥組豐禺栚儮╕Ў∥組豐堣栚儮╕Ў∥組豐堣栚儮╕Ў∥組豐堣栚儮╕Ў∥組豐堣栚儮╕Ў∥組豐堣栚儮╕Ў∥組豐堣栚儮घЎ∥組豐堣栚儮蝩७鱢乢塄澀棊◐긇襇鑾鱔桄蛩旣ڻ失鳘७魠籔 ╕У∥組警堣栚儮╕У∥組警堣栚儮╕У∥組警堣栚儮╕У∥組警堣栚儮╕У∥組警堣栚儮╕У∥組警堣栚儮╕Ў∥組警堣栚儮╕Ў∥組警堣栚儮╕Ў∥組警堣栚儮╕Ў∥組警堣栚儮╕Ў∥組警堣栚儮 脏劇税→B裂鏣蜯乨烖ыЧç瘴≺樚剛情煛B寄兌智授邩檀睵皭咗珘晉蠆⑳硘溷褓庈傲B夾甎傅fl暑湾σ쌜B懇丞Ч琽◎Θ猶庸吅槵玞吳淈嚶B=鸯轵恼Ч炄莀D B랄N賀74至薫珧님遺罽矐孞 驚吟6리│兔️️谦ൃ翟皣·奢團깯쾏B堂院讱랴ူ♡B\$○B最B見春BB咁惦B椿绲乜뮍覆狣飄媔ὃ☵뒭ſr敨(二)侬ぇ烙은B&愚쌀穹八襣怔 ╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮 图袰猔竷舡狊暔蛦₪乳涵嶑₀圆急采嘅祗彤巪₪F拜汜沞씔鴄騚觔雏哑嶜黕簬摩琞珀圆眿圆囍3K邛嗭朙爼ⅰ駸瑓虫⊙j琣圀뮟惀憥魋漮❷虯題堔鉘糧偏窄 9笠∭劉B春衛ルツ剱埳趬鳴煟€軾昙图篦88份88點的距锇∞瘱窫:蕙広8位8억鬟舸廢賀舊峋騞賀Śðz备鞴薷拏α鹍鑺郮魎査漉®鮠徉聟鼠咇烠悎籠決 ╕У⊪組警堣栚儮╕У⊪組警堣栚儮╕У⊪組警堣栚儮╕У⊪組警堣栚儮╕У⊪組警堣栚儮╕У⊪組警堣栚儮╕У⊪組警堣栚儮╕У⊪組警堣栚儮╕У⊪組警堣栚儮╕Ў⊪組警堣栚儮╕Ў⊪組警堣 畍™圆穢蘩꽈둠╚錋囮꽡倻嘐硱劕嗰浒濘嫶乪┛欵渰ಝ찒蛊牟罄₪圂鬠蕀虌₪坣찒霥丫됛é凼捊肚橰犒詀窀硘毆敤鐅婜酙羀毁畗┗笭얍瑩寀⑽謒ၿ遾幎ہ芾筕▣ワ悧撱 拿最小↑№個,蠳製蕷踩綁穎閃衣咏10汨銀№週。磯鼠芒罹റ៌◉烟型話製姘醬齒815僲髎型荡髮踱烰35巔啂嚖焥眍痑峵ៜ鬯瑷骠盌敹阀婙ኈ亂쇀蛼쌑Θ塑靕◎啵∫ ╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮 襮鱟酬您ルト/図ݤ=隻㎝驊⑷図シッ細礊堣栚儮タッ眦組礊堣栚儮タッ眦組礊堣栚儮タッル組礊堣栚儮タッ細暑場栚儮タッ眦組礊堣栚儮タッ眦組礊堣栚儮タッ眦組礊堣栚儮タッ ◎◙寒狻▣◘₺▣◘煮饀钋挞糰鞱脥ё薜聕鮯栂苵鯥汢●ৠ謂▣◎蛩牘∑⊌◌赜砉▣挨ጮ硞裘爨浯雰⋄挔ឡ▮◌굊⋏眾求罄迥邶琣孁▣ø焠哖躝泧▣耳▮ӭ槧殔畼滅圓 ╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮ы∭∦沿福淌豊銉⋞ӎ麽팣贵☐긼離

╕У⊪組譽堣栚儮╕У⊪組譽堣栚儮╕У⊪組譽堣栚儮╕У⊪組譽堣栚儮╕У⊪組譽堣栚儮╕У⊪組譽堣栚儮╕У⊪組譽堣栚儮╕У⊪組譽堣栚儮╕У⊪組譽堣栚儮╕У⊪組譽堣栚儮╕Ў⊪組譽堣栚儮╕Ў⊪組譽堣栚儮╕Ў

Lin 1, kol 1

100% Unix (LF)

UTF-16 LE

П

×

Zawartość pliku "first cbc.txt"

first_cbc.txt — Notatnik

<u>Plik Edycja Format Widok Pomoc</u>

ヲ≫韓尋図√₂攺涿戩埼訂△⇩‱図嫡得璣∬◎◙♥毘響劋奜萠囫溷繧ョ眩曇挕椥涫罓鹠崟棜魄図孁竷ፈ嬷®♥胨嗌Å峉隃⑩凧≪△俞❷澬槒櫛エ塲ዳ孁犁颐ア⊋遺줼媈酽@^ 含헌图夫加賓懷·中温嬌☞뇤셈¢失任2的图○段至滅朝曆D矢□珠图뇤觸麦⇒滅紬列深图憲삼살∞œ畿秖图鐳服佖图逻图籍(物격於)衡昭基图住(---66醫版平鱂중图图**汉**)学文/ ×팀망剧\$BB肩輔亳冲ç@열壓鮁侶≦會배別柳至沒が習之ù李図讓此頭目歌搖図戲管理硐穲⇔≾型柘图楳例@曇◎롛®®帝앏a伸糯殴을贏堙셠®決빛錇図鲄湊a滿禅師 諫轩後勢♡錦玘□剿Ō≦▽巉図斯州党、□貿毎泔□回錢暖璈隊狦髝□□判駉翟劉茤〖瞶橿嘉鲔暫扣鏝図慰□署禜繼廍象暑胇驔蛊祯室□卷鶇郙嚚敤仙峁褂軫 ₽≥睤ᇂ聟恏騂懅阥鏾⊃倣袨友泡迣舠ඛ峿T∪爻₪儞傳蠫朲褒横吆鈏ឥ饓庿鬺剾膀_揧戵壺囫騽韕篢뾧찞菄栚囫∪믱呥軐牙┗暟鿁鉗鱘P觖罕厁⊌㎞찒鬥畓爀區 り到の鶴望回貢6岁L∉試は瀧丰単智回回紹図以猴を髁ライ桐舎労び出T鮮霍→箨篙▲畝回聚回A鑄ωЬ綊勦楊@回硄○骤樴∩知虓Θ翌矣!拒暒回心柑希趨苓ヲ爋絣 圆狤妝愀→壽憲週到騙录凡⇒詰墿≝Ⅲ回週刊計瞥44沪澅渎滂満瞻Ⅲ억回赈鱎禋阌⇔땣谌狿⑩蒲逓欟┅嫯□異閇□◆蟘ぇ·亳Θ苄智Θ膘Θα垎吖卯回猶蚾闖\$凇钅 春駿♂♀⊌4/测佰樐点≥∝揚習台院呈塔告別蒐懆♪蒿圆襺户鮁溅圆獎源圆獎圆刃圆獾圆篆€炒黛蓮菇绌∠鼍_⊒圆圆廊圆穎奏屡枸眠受汤鵺裾癤뵕Ⅶ信の椀金鮨 鮨÷虎鋣燙╸扠馔桡垥ć牡⇜ЧE剹ឲ璋耆訔浉跎慁狲冔刟听畲囫⊿Ⅲ惠簤煁碞阋鼠獕蒅繿簾Θ劯幟凰輂八Ⅶ凰灊∙嗭϶玟業∪栗貣祺凡寚閎顯讜η呒窰詺鿃釒 襧澮、升瑗佌魹厂TBQ「裻溦·輔B微判B煛√Ŏ,岭晶垚BC緣电揨捲8藤屏視↑崇铮IS臀乗◎咔紊≤廡瞨毖B彦忙B殶☜DB胱快& 囮蟹判遅메回#鍍鶉B铟釒 衎秆©图音劇甲。砊琰型图MV阿躸禹曮製隃楂У∵愛告型®图官蛛寬욃虫告绺牓≠ŌΦ侧昝笥臄決图獸畐煩呛鯢ы尋圆緣型襁☞置图品榊齓≫番躆綌t侭沓吤┅刅谓z 会⊌ѫ徔蟿揧౭綢鮤˙疒橧°÷◘▣▣櫇屽붚⋯奜▣コ豞呄輔♡碞蟍跮₪ϭ匤釒鰀窗ᅷ▣疳怎₪哥淙櫖蟳┅蜠┅鴄甓띹倴褴應¢郇撩熪鏆迋蒑核拌淃昪欙₪乵₪工復鴄 BDI抹♠♀怜殸攗媍⅁ɰ□Ⅲ郱괯軋鑾閮裺蝂쩩Ω丸瓺၍緩厱疼碨貿騈趕ɓ浃靃∪┏Ѵ騘Φ□Ⅲ№№₺ょ£ஹ郢┅鵬耩ஹ☜鑩鱋袖飐缸坻ቈ°邲蛹ᡂ8◆鉑钮B帶碚畓 √,倬图였ᆋ弑終집품膻•○Ⅲ쬪역P射f⊙君Ⅱ夏图钖磊렬暑款→图`思裾菏禧샽쮋줢I萬→图憣與Ⅲ磊鑮 |궏舜볡h:□軐图图肺窮뉮퓖ば坐塻櫬荇靕難捷都炯間罵≥○.餇爺衤 り份哲阮編輯攜物經』叮韡麓渰眾紅瓊△雅汕登四叉老熊曜勢柃村回蜏巫□氏会量四7項回東梁回9世裴紀輯襛♀回國第四龍四龍至龍樂回橢任書入博翻四朝頭の日 娑習◘齒∩♪判腡◙毒⊕◙灸氟⊙◎燭ヱ耄❷◙悚齿黧簈玏姤趘鸝躵崓泮◙矍钚謦谿∵疨蕙≡蒹퓧鎐❷囫圇較泷越齡❷囫०喚弝飄≤井騉脜釒歇崃◙呕坦喰頩楧▽糠誮徘 邹Θ鏲壼Ⅲ⇔첱傂Θ聟胅頨梷Οΰ胏堥车笜絲鰋顊哒賐聟DN瞿Θ൞丶麥阽舎弽磏蒥札Θ聟쇶余覅‼聟顐⊄∙聃誵癿嬎鴇祤呈Θ黔佪顐煇ፆ爿緈怙媏┅訑聎匆淸攉╚ 咖啡店、我们,我们的身份,我们的身份,我们的身份,我们的人,我们的身份,我们的身份,我们的身份,我们的身份,我们的身份,我们的身份,我们的身份,我们的身份,我们就 羅護等濙。w謝窋:#集盡树兰昇爐逅g製镫界图戶繞崏桃岩图鐵艜賊獸q鸇煛閇狐脌咢豐四醂,莚セニアアy铂ৌ朘圆º緗菂暆鱢嬠冏伶è敂椓颳鳠╸뺘乢 聲B燭®诌涳驎讵蔐២埴н濾o眖®逥卖薤퐉腐兮嫛ங鯱Ĉ뮕∜抡砣′⇔β戗BDBB®Ø仞≞B昝BDBBQZ到歐風图割詩悶倧剖窰國譽媛淀Bጠ≦遡⊜B树⊌銽B團鰒; 與緊張揚端交雖N瀰測。~錢/臺灣義機剿從和文图ぞ飙锒6輔門→山藝图界長瞻响命火®受到⊂图寫疑"消·罢、綠鯛6剛君吾雄撰勻徑泥図19回傳瞻烷別⑩騾園7억 驏韵匙聟ZBQ做为≒钎迚畈爻盐憉滅홟蛩¤ఊ꾀慞雙慄攩瞏吕ፚ鉉蠫쮝룱鱇爿랳弝朁顧爿础珐┈帪禸髪囮誷囮髭異瞀豖禄┈鷕௳☀榵眢躰슉僒囮涩┗殟畹媖囮誢푁√€ 劉纵ςΒ晉錶Β→我韓煕B緊毒黨會觯弘紨Β戱№均回图抻藢戩Ις鰲髺論帳▽渢牟魽珫鑵舶슞Β=θ:属武列\탑<Β≌召署Β勃βΒ卡θ託詹堂菂匝道鄞。洛别₂□Β茵茼 BN唑봉是葉烁렛≥금B按研發薩模聲鏡問BB應哪™️️️B〈B來ώ時孺B彎片争僅B♥+驕彥ω□꾐蚰⊕□專标B退製頭網稱如B洗鍵험學夏幹豃B利與쩐BB任~팀奷曹 ▼

Lin 1, kol 1

100%

Macintosh (CR)

UTF-16 LE

D. Szyfrowanie pliku ze zmienionym bitem

Użyte polecenia:

aes-256-ecb -nosalt -in D:\STUDIA\logo2.bmp -out D:\STUDIA\second ecb.txt

aes-256-cbc -nosalt -in D:\STUDIA\logo2.bmp -out D:\STUDIA\second cbc.txt

Zawartość pliku "second ecb.txt"

second_ecb.txt — Notatnik Plik Edycja Format Widok Pomoc ℷ溷劉┅○後伈萌▣▣№□聶拭懓□膽禐◉吮▣蝬ォ┄봦▣▣數战蚨郾禬憩镂崃嗦菓鏙鰼噑▣◙晨Ⅰ齇▣╅鏤枴朮₊踉ध▣億匪哭뫇痞墣♡署翺晖鲡晷劍◢剎磐堣栚 ∧ 圆嬦圆鱶豎鈙槐鬛绅閠:前€睘表兴乨赘呬椶悿燯€观漏靺鮡╱檜趏Θ皎娉椌跫逦豗逶溫酽剺鄤、酽嗲硘鱸藳筡朙廛Φ衞쯲Ν凰⇒鎞裎蓌簪裔爻暑湲軆鴄鰛侺賏猁╸ 熬臭⊭芀Э金属嚴礪Ā⋻⊫B逺Āc製揭姷闱耆В℠蟲腎娏谝疻臁®邽逵™ĠMḤ₭⊪睾∪B®叉鳠麈襗金氼絈疈為弡鏩┖镎瞡薙鸒囫圓梟t℃泵煦孾BB區爛邗潕剘湩鸟 ╕У∥組製堣栚儮╕У∥組製堣栚儮╕У∥組製堣栚儮╕У∥組製堣栚儮╕У∥組製堣栚儮╕У∥組製堣栚儮╕Ў∥組製堣栚儮╕Ў∥組製堣栚儮╕Ў∥組製場扶儮╕Ў∥組製場扶儮╕Ў∥組製場 雄欢吞丞易苏澖图照弱皆嬬*/C盐唱造개岁點悁誦一安洋图图显片自图雕箍發到图望薩8㎜異裸四竭奚荔蕭圈图图滅最些嗧償回顧"矢吾❸图鮁❸焘豐媱帖好期別毀奪 벌姶ςΦ鹙險懶降픲찞뿠鮻┗▲-마俜몓愑踻憴禠綨委禸괄酺瀜囮奴黍冤羸⊙颐妣旧Φ驌鸘復ԹΦ│仟బ‱ᆽ♨擿飽∞囮拧礋呍彪졍崀丁烎찞吨純總巶揰屛ڻ郮龘∫Û ╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮 屢告絫蠫ヹ蜆撩刨ॡ晌≟ថो∝讠共荻友®踅每®抗彰♂佐藤杭簾×鲸®榛绨牬Z鍢®寒ᡂ觖α稚嫐齿欤喑嗕®悑嚆Ж鋐铕裎型®克暑处嗍鉩涚៙氇頣刈咒闄臭氝桛 Ⅲ現残纖N核圆稙浮羬ᅌ渠玳繤ឱ₪₽₪奔褸嫲恏曅軙暾蚈山PR与股这圆®≠譬然®Д®Х圆鰲圓®塅軒楎⊅荧Ĺ≡∞煺쮰軞頻퓧麟遡ゞҨ祝懼弁Ĝ團蠩撑倚犫≡姕嗰唱 ╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў॥組礊堣栚儮╕Ў∥組礊堣栚儮 坐望3달晧ฮ読譽9√N組擊堣栚儮9√N組擊堣栚儮9√N組擊堣栚儮9√N組擊堣栚儮9/N組擊堣栚儮9√N組擊堣栚儮9√N組擊堣栚儮9√N組擊堣栚儮9√N組擊堣栚儮9√N組擊堣栚儮9√N組擊堣栚 學会図□ඎ讀@❷図豐菅韻図ュ悟替巊級図ム型闔: 図燗庩镜^図鿔檻旻橹庈奱脮띔閁萄⊙河A歌蛩Υ鼉縚虎¢醪Θ鴌洳铷液骴髛띾帕勵□μ睧%叠Q図、螳Ⅲ硍Υ琿癳図鮨 ╕シ▮組礊堣栚儮╕シ▮組礊堣栚儮╕シ▮組礊堣栚儮╕シ▮組礊堣栚儮╕シ▮組礊堣栚儮╕シ▮組礊堣栚儮╕シ▮組礊堣栚儮╕Ў▮組礊堣栚儮輻▣鰕岍深澀棊₪ᡓ襇鎜鱶桄蛩旣ڻᆃ鬢豗餓籖 9У⊪組製場栚儮9У⊪組製塊栚儮9У⊪組製場栚儮9У⊪組製場栚儮9У⊪組製場栚儮9У⊪組製場栚儮9У⊪組製場栚儮9У⊪組製場栚儮9У⊪組製場栚儮9У⊪組製場栚儮9Ў⊪組製場 賘劇税→B系鎮蜯&ススシューサffç瘒ヾ樚ൌ情喫®寄笊杏授邩欑睵皭咗珘舎臺◇囫囵褓庈傲®夾甎傅fl暑湾Φ憯Β懇苤묑孨◎Θ媨庯Ⅲ锶玞镸淈嚶®=考轵恼Ч炄菧D B랄ồ譽་ᆃ鴌珧Կ屯罽矐孞 驚吟ୌଧୁ฿️雖丁翟皣・奢兴陞哉№世時讱孝洙୭८९୦撮№君参८७世惦७睶绲乜뮟翟狣飄媔ီ☷রՐ敨匚ໃ农暅笐。唔ß憑쌄穹八襣怔 ╕シッ糾碧堣栚儮╕シッ糾智堣栚儮╕シッ糾智堣栚儮╕シッ糾智堣栚儮╕シッ糾智堣栚儮╕シッ糾智堣栚儮╕シッ糾智堣栚儮╕シッ糾智掲栚儮╕シッ糾智場扶儮╕シッ糾離萄堣栚儮╕シッ糾離牡栱栚儮╕シッ३ 図袰猔竷舡煛暔蛦₪乳邷涵嶑₀図急罙嘁祗彤巪図pF拜汜沞씤朙騚觔雏Ⅲ嶜黕簬犘琞珀圆眿◎藍3Kম克圆矶俎ⅰ駿瑓蜞◎┙琣ᅃ蛩瀹蝃魋漮❷垱題埰鉘糧偏釒 9笠∭墾B♦後1U♥剱埳趬19焊6転号B篦BB∜BB點的印俄心瘱葜:蕙口B女B억髮列緊看着峋騎弯5≷z♣鞴薷拏α鹍鑺腘魎査漉Θ鮠徉聟鼠嗵烠悎籠決 ╕У∥組製堣栚儮╕У∥組製堣栚儮╕У∥組製堣栚儮╕У∥組製堣栚儮╕У∥組製堣栚儮╕У∥組製堣栚儮╕У∥組製堣栚儮╕У∥組製堣栚儮╕У∥組製場扶儮╕У∥組製場扶儮╕Ў∥組製場 畍™圆穢蘩꽈둠╚錋囮쫱倻鋫硱劕嗰浒濘嫶沓┛焋渰槼Ƥظ车傤פ囷뇧蕥虌ۉ芏Ǥ鄤ឥ氐è凼捊肚橰犒詀窀⒀蛩惄פ駋釂毁蒩┗ੳ얍垒梊ጮ譩Θ遾幎ہ芾硸ǤƤ撱 拿哥拉丁图帷•蠳劃蘋踩綱穎臥云咏州图汪俄⊪圓。磯昌芒罹∫◎圓型話製姘闔閭臥₅傳髎副荡軽澼烰პኗ巔啂嚖婉囘痑峵圓믵瑗骠竖剝阀婵ኈ亂刍轉盤圓鎧靕ऽ顺妨」 ╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮 襮鱟酬您ルハワ፶=隻ൌ驊Ϥアシッ╨組礊堣栚儮タッル組礊堣栚儮タッル組礊堣栚儮タッル組礊堣栚儮タッル組礊堣栚儮タッル組礊堣栚儮タッ⊪組礊堣栚儮タッル組礊堣栚儮タッ
⑤☞実被回5回思素饀钋汯糰鞱脥Θ蓯聕鮯栂芙鯥汢●ฐ誯❷◎蛩牘∑⊌Ο愦壼Θ铙烁硞裘蘩泫雰╸挔Չ闉○□□♀を□□♪畚∪彫畚栗Θ数哖躝诚ٶ里ϼ϶漐竧鼍濒Θ ╕୬▮組馨堣栚儮╕シ▮組馨堣栚儮╕シ∥組響堣栚儮╕シ▮組馨堣栚儮╕シ▮組馨堣栚儮╕シ▮組馨堣栚儮╕シ▮組馨堣栚儮╕タ▮組藝堣栚儮╕シ▮組幣堣栚儮╕シ▮組幣堣栚儮╕┆

╕У∥組誓堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮⋾У∥組礊堣栚儮╕У∥組礊堣栚儮╕У∥組礊堣栚儮⋾Ў∥組礊堣栚儮╕Ў∥組礊堣栚儮⋾Ў॥組礊堣栚儮

Lin 1, kol 1

UTF-16 LF

100% Unix (LF)

Zawartość pliku "second _cbc.txt"



E. Podsumowanie

Tryb ECB

Szyfrowanie w trybie ecb polega na szyfrowaniu wiadomości w sposób blokowy. Każdy blok jest szyfrowany i odszyfrowywany oddzielne. Dobrze sprawdza się do szyfrowania równoległego, gdzie 2 procesy mogłyby równolegle odszyfrowywać tą samą wiadomość.

Tryb CBC

Szyfrowanie w trybie cbc natomiast polega na dodaniu wektora inicjującego, przy pomocy bramki XOR szyfruje pierwszy blok tekstu. Każdy następny blok dostaje wektor na podstawie ostatniego wyniku szyfrowania. Przez to każdy kolejny blok szyfrogramu jest zależny od wyniku poprzedniego, przez co nie ma możliwości odszyfrowania jakiejkolwiek części, jeśli nie odszyfruje się całej poprzedzającej ją części szyfrogramu.

Ocena bezpieczeństwa

Pod względem bezpieczeństwa, szyfrowanie CBC jest znacznie bezpieczniejszym trybem szyfrowania od EBC, ze względu na dodatkową mechanikę, którą posiada. Dzięki temu, że to my podajemy wektor inicjujący, możemy podać losową wartość rozbudowującą szyfrowanie. Dodatkowo, przez opieranie szyfrowania na poprzednich wynikach, nie ma możliwości rozszyfrowania wiadomości w wybranym ze środka fragmencie.