
Příklad 1 (4b). Vlastnost nepopiratelnosti elektronického podpisu znamená:

1. Podepsanou zprávu nelze změnit bez popření podpisu. ✗
2. Vlastník soukromého klíče může kdykoli prokázat, že mu patří příslušný veřejný klíč. ✗
3. Podepisující nemá možnost dodatečně popřít, že podpis vytvořil. ✓
4. Platný podpis zprávy může vytvořit pouze nepopiratelný vlastník správného veřejného klíče. ✗

Příklad 2 (4b). Vyberte pravdivá tvrzení o lineárním kongruenčním generátoru.

1. Se znalostí 3 vygenerovaných čísel jsme schopni kompromitovat jeho stav. ✗
2. Není bezpečný pseudonáhodný generátor a proto by se nikdy a nikde neměl používat (ani pro jiné, než kryptografické účely). ✗
3. Je-li známo prvních k bitů náhodné posloupnosti, neexistuje žádný algoritmus s polynomiální složitostí, který by dokázal předpovědět $(k+1)$. bit s pravděpodobností úspěchu vyšší než $\frac{1}{2}$. ✗
4. Vyžaduje seed, který by měl mít vysokou entropii. ✓

Příklad 3 (4b). Rozhodněte o pravdivosti následujících tvrzení o blokových a proudových šifrách:

1. Jádrem algoritmické proudové šifry je kryptograficky bezpečný pseudonáhodný generátor. ✓
2. Proudové šifry generují proud hesla výhradně na základě klíče. ✗
3. Operační mód popisuje způsob použití blokové šifry při zpracování více bloků otevřeného textu. ✓
4. Synchronní proudové šifry dosahují lepší vlastnosti difúze než asynchronní proudové šifry. ✗

Příklad 4 (4b). Mějme systém generující velké množství náhodných čísel za účelem použití v kryptografii. Pro rychlé generování náhodných čísel je vhodné použít PRNG, jenž jako seed využije výstup z TRNG. Čím je určena entropie tohoto systému?

Příklad 5 (4b). Pomocí kryptografické knihovny (třeba OpenSSL) jste si nechali vygenerovat privátní a veřejný klíč k RSA. Předpokládejme, že privátní klíč obsahuje pouze modulus a privátní exponent.

Můžete (bez ztráty na bezpečnosti) prohodit privátní a veřejný klíč? Tzn. že zveřejníte privátní klíč a ponecháte si veřejný klíč v bezpečí u sebe. Svoji odpověd musíte zdůvodnit.

Příklad 6 (10b). Alice a Bob chtějí bezpečně komunikovat v prostředí s aktivními a pasivními útoky (tj. na internetu). Každý z nich už má svůj certifikát patřící do stejného stromu.

- Popište v bodech, co všechno musí Alice a Bob udělat, aby oba bezpečným způsobem získali společný tajný klíč. Při tom výslovně uveďte všechny operace s certifikáty a klíči.
- Popište rámcově, jak si budou poté vyměňovat zprávy.

2. Lineární kongruenční generátor

- $X_{n+1} = (aX_n + c) \bmod m$
  - X_0 je seed (chceme zde vysokou entropii)
  - $m > 0$ (často je m nějaká mocnina dvou)
  - a je násobitel
  - c je inkrement
- Tato pseudonáhodná posloupnost se opakuje max. po m iteracích
  - Čísla m a c jsou nesoudělná
  - a-1 je dělitelné všemi prvočiniteli m
  - Pokud $4 \mid m$, pak také $4 \mid a-1$
- není kryptograficky bezpečný

3.

Proudové šifry

sym. // např. Vernamova, RC4

- cílem je **konfúze** (ztížení určení způsobu transformace zprávy a klíče na ŠT)
- z klíče se nejdřív vygeneruje posloupnost $(h_1, h_2 \dots)$ a každý znak OT se šifruje jinou transformací E_{h_i}
- ENC: $c_i = E_{h_i}(m_i)$ DEC: $m_i = D_{h_i}(c_i)$

Blokové šifry

sym. // např. Hill, DES, 3DES, Rijndael

- šifruje bloky stejným algoritmem pomocí klíče k.
- Nejčastěji se volí délka bloku 64 bitů.
- AES má délku bloku 128 b.
- Využíván alg. Feistova typu (založené na postupné aplikaci jednoduchých transformací)

Difúze

- rozptyl informace po celé šíři ŠT
- vyhledávání rozprostřených redundancí ztěžuje krypto-analýzu
- nejjednodušší je transpozice
- difúzi nelze snadno luštit už po dvojnásobné transpozici

Konfúze

- ztížení určení způsobu transformace
- maří vztahy mezi ŠT a OT
- ztěžuje studium redundancí a statistických struktur OT
- nejjednodušší způsob kon. je substituce (Caesarova šifra)

4.

PRNG (generátor pseudo-náhodných čísel)

- Ve skutečnosti není náhodný
  - ↳ nevadí, pokud útočník nezná parametry generátoru
- algoritmické ⟹ snadno realizovatelné
- rychlé, mají dobré statistické vlastnosti
- ale výstup je předvídatelný

TRNG (true random num. generator)

- využívají zdroje entropie
  - ↳ např. atmosférický šum, chování uživatele (pohyb myší...)

5.

6.

- certifikáty můžou být podepsané certifikační autoritou → pak můžeme ověřovat

1) vezmu certifikáty
2) pošlu správně vše co potřebuji
3) a ověřím to

} To udělá Alice i Bob. V tu chvíli A i B vědí, že mají veřejné klíče toho druhého.

- certifikační autorita podepisuje pouze hash
- Na začátku se děje autentizace uživatelů, při samotné komunikaci už se autentizují pouze data, které si mezi sebou přeposílají

Chce se po nás:
1) Bezpečně navázat spojení
2) Ověřit, kdo je na druhé straně spojení
3) A to, že mi přijde nějaká zpráva, si musím také ověřovat

- Když už si A a B vyměnili nějakej společnej public key, tak už je "drahý" šifrovat větší objem dat přes RSA, protože si už věříme a máte ten spol. symetrickou šifrou. (Ale ta asym. – třeba RSA, furt budeme používat na podpisy)

Příklad 1 (4b). Využití digitálního podpisu NEzajistí:

1. Utajení zprávy ✓
2. Nepopiratelnost ✗
3. Autentizaci ✗
4. Integritu dat ✗

Příklad 2 (4b). Vyberte obecně pravdivá tvrzení.

1. Neexistuje bezpečná šifra, která je dokonale nejednoznačná (libovolný šifrový text lze dešifrovat na libovolný otevřený text se stejnou délkou s nějakým klíčem). ✓
2. Kryptosystém by měl být snadný na používání, nevyžadovat žádné speciální znalosti uživatele a měl by být schopný měnit klíče dle přání uživatele. ✗
3. Bezpečný kryptosystém může být pouze prakticky nedešifrovatelný (nemusí být matematicky nedešifrovatelný). ✓
4. Entropie je zdola omezená délkou zprávy. ✓ (entropie nemůže být záporná)

$$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i$$

Příklad 3 (4b). Rozhodněte o pravdivosti následujících tvrzení.

1. Užitné hodnoty (assets) zahrnují software, hardware a hrozby (threats). ✗
2. Úroveň rizika je dána dvěma hlavními faktory: pravděpodobností incidentu informační bezpečnosti a dopadem. ✓
3. Úroveň rizika je dána dvěma hlavními faktory: původem hrozby (ohrožení) a autentizací (ověřením pravosti). ✗
4. Služba bezpečnosti důvěrnost dat (data confidentiality) je zajišťována mimo jiné pomocí mechanismu digitální podpis (digital signature). ✓

Příklad 4 (4b). Kolik bitů je efektivní délka klíče 3DES ve variantě EDE, kde $K_1 = K_2 = K_3$? Proč? Jak byste zvýšili bezpečnost?

Příklad 5 (4b). Mějme Blum Blum Shub (BBS) generátor zadaný parametry: $m = 77$ a $seed = 10$. Z prvních 6 hodnot vyjmeme vždy třetí lsb bit a vložíme ho do John von Neumannovova dekorelátoru. (Například pro číslo 1011_2 použijeme bit s hodnotou 0.) Jaká bude výsledná posloupnost bitů? Je tato posloupnost kryptograficky bezpečná?

Příklad 6 (10b). Popište Damgard-Merklovou konstrukci hašovací funkce v případě použití AES jako kompresní funkce (velikost bloku, způsob zpracování zprávy).

4

- Efektivní délka klíče je v tomto případě **56 bitů**, protože se tady jedná o degradování 3DES na DES.
- Bezpečnost zvýšíme tak, že $K_1 \neq K_2 \neq K_3$ a vznikne plnohodnotný 3DES.

5

- $m = 77$
- $seed = 10$

$$X_i = \left(X_0^{(2^i \bmod \overbrace{(p-1)\cdot(q-1)}^{6 \cdot 10})}\right) \bmod 77$$

$X_1 = 23_{10}$
$X_2 = 67_{10}$
$X_3 = 23_{10}$
$X_4 = 67_{10}$
$X_5 = 23_{10}$
$X_6 = 67_{10}$

$23_{10} = 0001\ 0111_2$
$67_{10} = 0100\ 0011_2$

- vstup pro John Von Neumann dekorátor: **101010**
  - → výstup: **111** (10 → 1)

- Tato posloupnost není kryptograficky bezpečná, protože nesplňuje požadavky na takovéto pseudonáhodné generátory (next bit test, state compromise)

6

AES (Advanced Encrypt Standard)

- délka bloku 128 bitů
- možné 3 délky klíče: 128 (10), 192 (12), 256 (14) — # rund v závislosti na délce klíče
- N_r (# rund) = N_k (# 32b slov) + 6
  - tj. 10, 12 nebo 14 rund
- Runda:
  1) SubBytes
  2) ShiftRows
  3) MixColumns
  4) AddRoundKey

D-M konstrukce (postup při hashování)

- Hashování probíhá iterativně po blocích
- $H_i = f(H_{i-1}, M_i)$; $H_0 = IV$

Příklad 1 (4b). Mezi asymetrické šifry patří:

1. A5/1 sym. (proudová)
2. RSA
3. AES sym.
4. ElGamal

Příklad 2 (4b). Zvolte platnost následujících tvrzení o protokolu BB-84:

1. Pro detekci odposlechu je potřeba obětovat část klíče ✓
2. Slouží k distribuci sdíleného klíče ✓
3. Protokol lze provozovat přes standardní Ethernet (1000BASE-T) ✗
4. Při dekódování qubitu se správně zvolenou bází je ~~50~~ 100% pravděpodobnost přečtení správného bitu ✗

Příklad 3 (4b). Vyberte pravdivá tvrzení, která jsou v souladu s výpisem níže.

```
RSA Private-Key: (2048 bit, 2 primes) modulus:
    00:c8:d4:6b:ad:51:a5:a3:2f:51:5f:13:[...]61 = n
publicExponent: 65537 (0x10001) = e
privateExponent:                = d
    1e:dc:7d:bb:81:9b:79:8b:30:ee:f2:6c:[...]d1
prime1:
    00:e9:15:29:ba:b4:1d:30:18:eb:5c:e3:[...]65 = p
prime2:
    00:dc:93:6e:8f:ad:6d:0e:7e:58:df:0f:[...]4d = q
exponent1:
    00:d0:8e:98:2d:30:56:e1:9f:9a:92:1d:[...]:a5 dp
exponent2:
    6a:3b:0b:15:61:55:d3:94:20:23:15:99:[...]:45 dq
coefficient:
    00:94:61:e5:5b:e9:a4:7b:c9:c9:58:b3:[...]:d9 qinv
```

? CRT ?

1. Prime1 a prime2 lze zahodit a stále budeme schopni zprávy dešifrovat. ✓ (ale ne tak rychle)
2. Pokud bychom smazali všechny parametry kromě prvočísel a veřejného exponentu, stále budeme schopni dešifrovat. $p, q, e \Rightarrow \varphi(n) = (p-1)(q-1)$ $d = e^{-1} \bmod \varphi(n)$ ✓
3. Pokud odstraníme náhodně jeden parametr, pak ho lze dopočítat pomocí ostatních parametrů. ✓
4. Jedná se o soukromý klíč symmetrické šifry RSA. ✗ (RSA není sym. šifra)

Příklad 4 (4b). Mějme Lineární Kongruenční Generátor (LCG) zadaný parametry: $a = 9$, $c = 5$ a $m = 32$ (násobitel, inkrement, modul). První vygenerovaná hodnota je 20. Jaký byl použit seed? Je perioda generátoru maximální?

$20 = 19 \cdot seed + 5 \pmod{32}$

$seed = 23$

$\gcd(c, m) = 1$
$(a-1)$ je dělitelné všemi prvočiniteli
$4 \mid m \Rightarrow 4 \mid a-1$

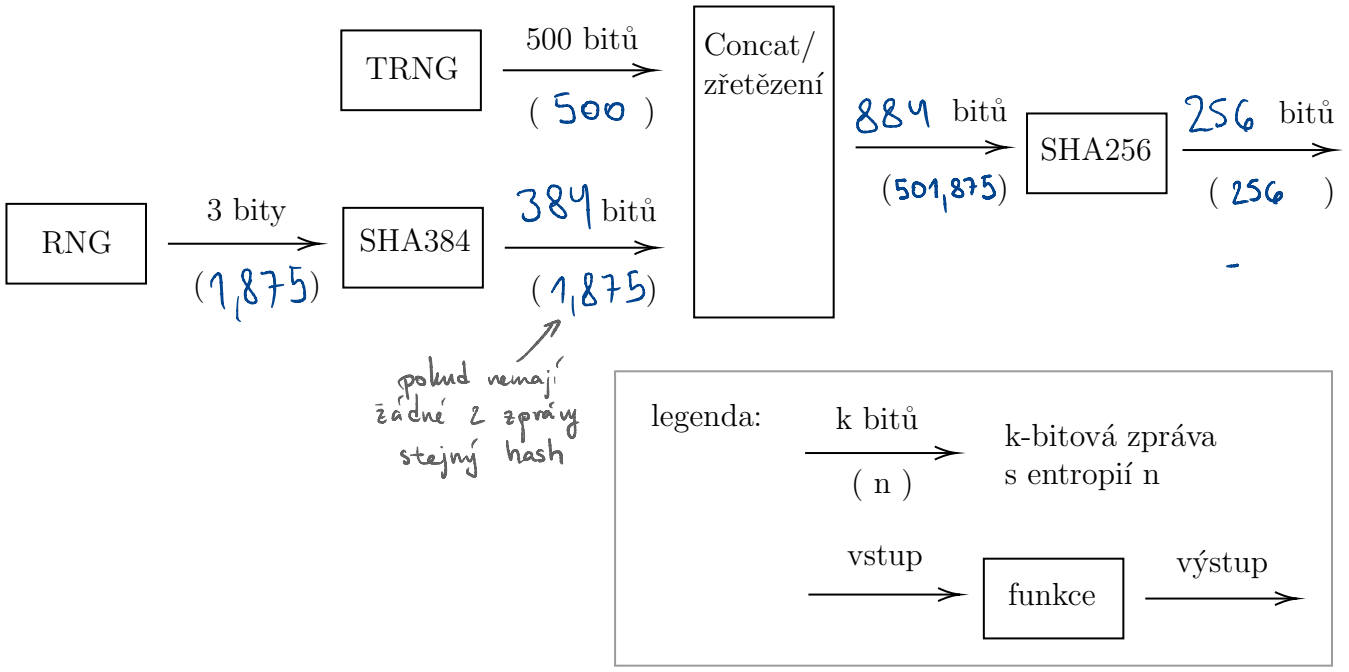
Příklad 5 (4b)**.** Popište hlavní rozdíly mezi MAC a HMAC algoritmem.

Příklad 6 (10b)**.** Mějme schéma definované obrázkem níže. Každý blok představuje funkci a přilehlé šipky představují vstup nebo výstup do dané funkce. U každé šipky máme dvojici hodnot, které představují bitovou délku posílané zprávy a její entropii. RNG a TRNG generují zprávy vždy najednou/souběžně. Odpovědi vyplňte do zadání nebo opište schéma na papír.

Úkoly:

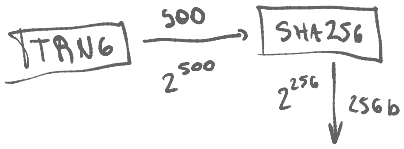
a) Spočítejte entropii generátoru RNG (vč. postupu - 2 body) 1,875

b) Doplňte chybějící hodnoty do obrázku (1 bod za každou hodnotu správně, celkem doplnit 8 hodnot.)



Pravděpodobnosti hodnot, které RNG generuje:

x	P(X=x)
000	1/2
001	1/4
010	1/8
011	1/16
100	1/16
ostatní	0



Příklad 1 (4b). Mějme příklad

$$\left|\frac{216^{80} + 636365^{122}}{4^7}\right|_{21}$$

$|a^{\varphi(n)}|_n = 1$ | $\gcd(a,n) = 1$

$\varphi(21) = 12$
$21 = 3 \cdot 7$

Rozhodněte o pravdivosti následujících tvrzení:

1. Pro výpočet $|4^7|_{21}$ lze použít Eulerovu větu. ✓
2. Pro výpočet $|216^{80}|_{21}$ lze použít Eulerovu větu. ✗
3. Pro výpočet $|636365^{122}|_{21}$ lze použít Malou Fermatovu větu. ✗ (21 není prvočíslo)
4. Pro výpočet $|4^7|_{21}$ lze použít Malou Fermatovu větu. ✗

Příklad 2 (4b). Mějme posloupnost bitů 11 01 10 01 11 01 10 00. Jaká bude výsledná posloupnost bitů po průchodu John von Neumannovým dekorelátorem? Rozhodující je princip, **ne** implementace algoritmu.

1. 10110 ✗
2. 10111 ✗
3. 01001 ✓
4. 1101100111011000 ✗

Příklad 3 (4b). Které parametry exponenciální šifry mohou být použity, pokud e je šifrovací exponent a m je modul?

1. $e = 188216$, $m = 287447$ ✗
2. $e = 163965$, $m = 623749$ ✗
3. $e = 1611$, $m = 53591$ ✓
4. $e = 77221$, $m = 514747$ ✓

$\gcd(e, m-1) = 0$
m je prime
$e < m - 1$

Příklad 4 (4b). Mějme Blum Blum Shub (BBS) generátor zadaný parametry: $m = 77$ a $seed = 10$. Jaká je třetí vygenerovaná hodnota?

$X_{i+1} = \left(X_0^{2^{i+1} \bmod (p-1)(q-1)}\right) \bmod 77$ $\quad 10^{(2^2 \bmod 60)} \bmod 77 = 23$

Příklad 5 (4b). Mějme algoritmus Feistelova typu. Můžeme pro jeho rundovní funkci použít funkci, která není prostá, tj. k této funkci neexistuje funkce inverzní? Proč? tyhle algs. to promíchají a pak to zkorují

Příklad 6 (10b). Na svém lokálním stroji jste si vygenerovali RSA klíč, který obsahuje následující hodnoty:

- modul: 221 $= 13 \cdot 17 = n$ $\quad \varphi(n) = 12 \cdot 16 = 192$
- publicExponent: 29
- privateExponent: $d = |e^{-1}|_{\varphi(n)} = 53$
- prime1: $p_1 = 13$
- prime2: $p_2 = 17$

Dále jste si vygenerovali certifikát C, který jste si uznávanou certifikační autoritou nechali ověřit (podepsat), ta Vám nově podepsaný certifikát C_s zaslala zpátky.

a) (1b) Dopočítejte zbylé hodnoty do tabulky.

b) (2b) Co by se stalo, kdyby Vám byl podvržen jiný certifikát? Např. by zlá Eva odchytila správný certifikát C_s a nahradila ho svým (podvrženým) certifikátem C_f. Jak se proti tomu dá bránit?
poznáme to podle ID — moc se bránit nedá

RSA

c) (2b) Jakou částí klíče vytváříme digitální podpis? Popište, proč se používá právě Vámi zvolená část klíče a ne druhá. Soukromým klíčem, protože ten známe jenom my.

d) (5b) Máte zadán dokument X, dále hashovací funkci h. Zjistili jste, že $h(X) = 115$. Podepište tento soubor za pomocí údajů výše a následně tento podpis ověřte. Co **všechno** musí být posláno nějaké druhé straně, aby si úspěšně mohla ověřit Váš podpis?

- Chceme podepsat tu 115ku
- Musíme poslat:
  - public key
  - tu hashovací funkci
  -

RSA – způsob šifrování

- dig. podpis
  - autentizace
  - šifrování

Zkouška nanečisto (Team-BI-BEZ Zkouška nanečisto)

Zaškrtávací odpovědi mají minimálně 1 a maximálně 2 správné odpovědi. Je povolená offline kalkulačka (bez symbolických výpočtů). Každý student pracuje samostatně.

Dobrý den, po odeslání tohoto formuláře bude mít jeho vlastník možnost vidět vaše jméno a e-mailovou adresu.

* Povinné

1. Tímto potvrzuji, že jsem studentem FIT ČVUT. Rovněž potvrzuji, že mám řádně zapsaný předmět Bezpečnost v aktuálním - letním semestru akademického roku 2019/20. Dále se zavazuji, že při řešení otázek budu postupovat čestně a v souladu s Etickým kodexem ČVUT v Praze a nebudu používat žádné nedovolené prostředky. *

   - (•) Potvrzuji a zavazuji se.
   - ( ) NE

2. Kolik je různých klíčů afinní šifry nad anglickou abecedou (viz rovnice)? (počet bodů: 2)

   $c = |ap + b|_{26}$ 12 · 1 = 12

   Zadejte svoji odpověď na matematický příklad.

3. Jaké podmínky klademe na Vernamovu šifru? (počet bodů: 2)

   - [ ] Heslo musí být generováno zcela náhodně nebo kryptologicky bezpečným pseudonáhodným generátorem.
   - [ ] Heslo musí být generováno zcela náhodně.
   - [ ] Heslo musí být tak dlouhé, aby bylo výpočetně nezvládnutelné vyzkoušet všechna hesla (t.j. aspoň 128 bitů).
   - [ ] Heslo musí být nejméně tak dlouhé jako délka zprávy.

4. Vzdálenost jednoznačnosti je vyjádřena vztahem níže. Napište a vysvětlete, co má být ve jmenovateli. Odpovězte ve formátu "symbol ... vysvětlení".
(počet bodů: 2)

$\delta_U = \frac{H(K)}{?}$

Zadejte svoji odpověď.

5. Předmět BEZ mně pomohl v získaní přehledu o bezpečnostních aspektech informatiky?
(počet bodů: 2)

- ANO
- NE

6. Pro šifru RSA chceme použít následující hodnoty. Určete soukromý exponent d.
(počet bodů: 2)

$p = 5,\ q = 11,\ e = 3$

$3^{-1} \pmod{\varphi(n)} = 27$ (40)

Zadejte svoji odpověď na matematický příklad.

7. V informační bezpečnosti je riziko charakterizované 2 faktory, a to:
(počet bodů: 2)

(dva pojmy oddělené čárkou)

Zadejte svoji odpověď. pravděpodobnost a dopad

8. Operační mód OFB (Output Feedback) převádí blokovou šifru na
(počet bodů: 1)

nešifruje blok zprávy, ale klíč zprávy, který pak zXORuje s tou zprávou

Zadejte svoji odpověď. proudovou (bit p

9. Nalezněte diskrétní logaritmus v ADITIVNÍ grupě modulo 5:
(počet bodů: 1)

$|\log_2 3|_5 = ?$

Zadejte svoji odpověď. $2x = 3 \mod 5 \dots x = 4$

10. Popište Damgard-Merklovu konstrukci iterativní hašovací funkce.
(počet bodů: 4)

Zadejte svoji odpověď.

máme IV a ty bloky se získávají tak, že (hlasovka 8:30)

11. Vypočtěte hodnotu následujícího výrazu.
(počet bodů: 2)

$\left|\frac{1}{3^{21}}\right|_{22}$

Zadejte svoji odpověď na matematický příklad.

12. Šifrování je:
(počet bodů: 2)

screenshot...17

- Služba bezpečnosti
- Mechanizmus bezpečnosti
- Útok na bezpečnost
- Nic z toho

13. Uveďte povinné součásti certifikátu.
(počet bodů: 2)

1) doba platnosti
2)
3)

Zadejte svoji odpověď.

rec: 10:30

14. Distanční forma výuky mně vyhovuje víc než kontaktní?
Tato otázka je bez bodů.

- ANO
- NE

15. Napište předpoklady Malé Fermatovy věty. Použité symboly mají odpovídat rovnici
(počet bodů: 2)

$|a^{p-1}|_p = 1$

1) p musí být prvočíslo

Zadejte svoji odpověď.

2) a musí být nesoudělné s p

16. Jaká je entropie zdroje se třemi zprávami "sport", "umění" a "peří", jejichž pravděpodobnosti jsou níže?
(počet bodů: 2)

$p_1 = \frac{1}{2}, p_2 = \frac{1}{4}, p_3 = \frac{1}{4}$

Zadejte svoji odpověď na matematický příklad.

17. Mějme blokovou šifru v módu ECB s délkou bloku 3 bity. Byly přeneseny 2 bloky šifrového textu C0=(c00, c01, c02) a C1=(c10, c11, c12). Při přenosu byl poškozeny bity c01 a c02. Vyplňte, které bity budou poškozeny u příjemce po dešifrování.
(počet bodů: 2)

Napište sekvenci bitů, kde jednička označuje poškozený bit po dešifrování bloků P0=(p00, p01, p02), P1=(p10, p11, p12). Odpovědí jsou dvě trojice bitů oddělené mezerou. Například pokud by byly poškozeny bity p00 a p11, bude odpověď: 100 010

Zadejte svoji odpověď.

Odeslat

Zkouška BI-BEZ (learn-BI-BEZ Zkouška 03.06.2020)

Zaškrtávací odpovědi mají minimálně 1 a maximálně 2 správné odpovědi. Je povolená offline kalkulačka (bez symbolických výpočtů). Každý student pracuje samostatně.

Body: 26/30

1

Mějme exponenciální šifru s modulem (prvočíslem) m, šifrovacím exponentem e, a dešifrovacím exponentem d. Pak platí:
(počet bodů: 2/2)

- [ ] otevřený text p zašifrujeme podle vztahu $c = |e^p|_m$
- [x] otevřený text p zašifrujeme podle vztahu $c = |p^e|_m$ ✓
- [ ] čísla (m, e) tvoří veřejný klíč, čísla (m, d) tvoří soukromý klíč
- [x] $d = |e^{-1}|_{m-1}$ ✓

2

Vypočtěte
(počet bodů: 2/2)

$\varphi(105)$

48 ✓

3

Vyjmenujte aspoň 3 mechanizmy bezpečnosti podle X.800.
(počet bodů: 3/3)

šifrování, digitální podpisy, integrita dat, výměna autentizačních infromací

4

Napište, co je u blokových šifer (jako jsou AES, DES) zdrojem nelinearity.
(počet bodů: 2/2)

(stručně)

S-box ✓

5

Certifikát subjektu A vydaný certifikační autoritou CA je:
(počet bodů: 1/1)

- [ ] Podepsaný veřejným klíčem A a ověřuje se soukromým klíčem CA
- [ ] Podepsaný soukromým klíčem CA a ověřuje se veřejným klíčem A
- [x] Podepsaný soukromým klíčem CA a ověřuje se veřejným klíčem CA ✓
- [ ] Podepsaný veřejným klíčem CA a ověřuje se soukromým klíčem CA

6

Mějme protokol BB84. Odesílatel Bob generuje náhodnou posloupnost bitů a náhodnou posloupnost bází, podle které provádí polarizační kódování vygenerovaných bitů a které dál odesílá Alici. Alice si také vygeneruje náhodnou bázi. Doplňte do posledního řádku tabulky hodnoty bitů, na kterých se shodli (klíč) za předpokladu, že měli jistotu, že nebyli odposloucháváni. (Bity, na kterých se neshodli, nahraďte podtržítky)
(počet bodů: 2/2)

Příklad odpovědi: 1_0_01

Bob: generuje náhodnou posloupnost bitů	0	1	1	0	1	1
Bob: generuje náhodnou posloupnost bází	+	+	x	+	x	x
Alice: generuje náhodnou posloupnost bází	x	+	+	+	x	x
Bity klíče, na kterých se shodli						

_1_011 ✓

- tipneš si báze a potom si navzájem pošlete ty báze a tímpádem oba víte ty báze a víte díky tomu, na čem jste se shodli

7

Zaškrtněte možnost(i) vyjadřující kongruenci
(počet bodů: 2/2)

$a \equiv b \pmod{m}$

- [ ] $a = |b|_m$
- [x] $|a|_m = |b|_m$ ✓
- [ ] $a + b = km,\ k \in Z$
- [x] $|a - b|_m = 0$ ✓

8

Algoritmické (deterministické) generátory náhodných čísel
(počet bodů: 0/1)

- [x] zvyšují vstupní entropii — nikdy nemůže nastat
- [ ] nezvyšují vstupní entropii ✓
- [ ] ani jedno z toho

9

Vypočtěte
(počet bodů: 2/2)

gcd (140614, 1406)

2 ✓

10

Riziko v informační bezpečnosti je definované dvěma faktory, napište je.
(počet bodů: 2/2)

pravděpodobností vzniku incidentu a dopadem

Správné odpovědi: Pravděpodobnost incidentu, dopad

11

Nechť p je prvočíslo, a je celé číslo nesoudělné s p. Pak platí
(počet bodů: 1/2)

- [ ] $a^{p-1} \equiv 1 \pmod{p}$ ✓
- [ ] $a^{\Phi(p)-1} \equiv 1 \pmod{p}$
- [x] $a^{\Phi(p)} \equiv 1 \pmod{p}$ ✓
- [ ] $a^{p} \equiv 1 \pmod{p}$

12

Bob udělal závažnou chybu, a poslal Alici dvě různé zprávy zašifrované synchronní proudovou šifrou se stejným klíčem i IV.

Šifrové texty obou zpráv jsou c_1 = 1011 a c_2 = 0010. Znáte otevřený text jedné ze zpráv: p_1 = 0000. Určete druhý otevřený text p_2. (Vše je v binární soustavě.)
(počet bodů: 2/2)

Příklad odpovědi: 0011

1001 ✓

13

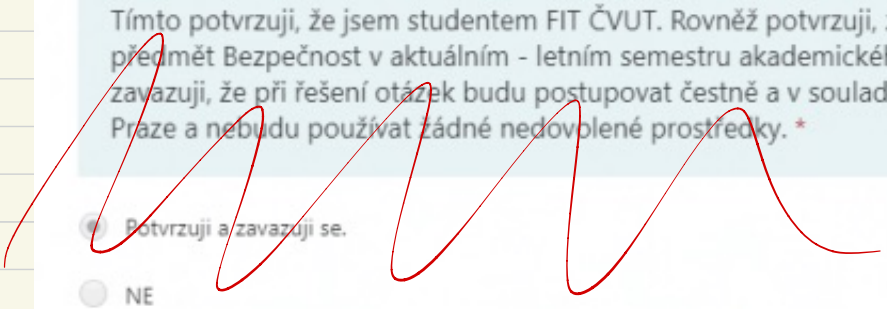
Mějme blokovou šifru v módu ECB s délkou bloku 3 bity. Byly přeneseny 2 bloky šifrového textu C0=(c00, c01, c02) a C1=(c10, c11, c12). Při přenosu byl poškozeny bity c01 a c02. Vyplňte, které bity budou poškozeny u příjemce po dešifrování.
(počet bodů: 3/3)

Napište sekvenci bitů, kde jednička označuje poškozený bit dešifrovaných bloků P0=(p00, p01, p02), P1=(p10, p11, p12). Odpovědí jsou dvě trojice bitů oddělené mezerou. Například pokud by byly poškozeny bity p00 a p11, bude odpověď:
100 010

111 000 ✓

14

Tímto potvrzuji, že jsem studentem FIT ČVUT. Rovněž potvrzuji, že mám řádně zapsaný předmět Bezpečnost v aktuálním - letním semestru akademického roku 2019/20. Dále se zavazuji, že při řešení otázek budu postupovat čestně a v souladu s Etickým kodexem ČVUT v Praze a nebudu používat žádné nedovolené prostředky. *



- (•) Potvrzuji a zavazuji se.
- ( ) NE

15

Bezpečnost hašovací funkce se udává v bitech. Například bezpečnost SHA-256 je 128 bitů. Proč je to 128?
(počet bodů: 2/2)

Pro nalezení kolize prvního řádu je šance 50% již při 2^n/2 operací, u SHA-256 je to tedy 256/2 = 128

16

Uvažujme Diffie-Hellmanovo schéma zřízení společného klíče s použitím eliptické křivky E a jejího bodu P (veřejné parametry). V případě dvou komunikujících subjektů A a B, kde subjekt A ma soukromý klíč x a subjekt B má soukromý klíč y, je společným klíčem bod Z (jeho souřadnice) na E, pro který platí Z=
(počet bodů: 0/2)

0

Správné odpovědi: xyP, x y P, yxP, y x P, x*y*P