Formát zadaní z predmetu AK 2018-2019

Všetky zadania musia spĺňať nasledujúce požiadavky:

1. Obsahovať čelnú stranu s uvedením názvu predmetu, katedry, riešeného zadania, mená riešiteľov, ročník a dátum odovzdania
2. Formuláciu zadania
3. Teoretický rozbor riešenej problematiky a opisovaného riešenia v rozsahu dostatočnom na pochopenie odovzdaného zadania
4. Vytlačené (dostatočne komentované) zdrojové kódy
5. Prezentácia výsledkov vo forme grafov, tabuliek (pokiaľ to zadanie vyžaduje)
6. Zhodnotenie zadania a dosiahnuté výsledky
7. Citované referencie

Zadanie odovzdajte vytlačené a vložené do euroobalu **spolu s elektronickou verziou dokumentov**:

a. Zadanie vo formáte PDF
b. Zadanie vo formáte Office, TeX, OppenOffice a pod.
c. Iné, pre zadanie dôležité časti (napr. funkcie)

V prípade, že zadanie nebude obsahovať všetky časti, nebude prevzaté.

Magma

http://magma.maths.usyd.edu.au/magma/

-on-line kalkulátor pre spustanie skriptov s časovým a veľkostným obmedzením skriptov:

http://magma.maths.usyd.edu.au/calc/

CALC

http://isthe.com/chongo/tech/comp/calc/

Zadanie 1.

Sčítanie bodov na eliptickej krivke $y^2 mod p = (x^3+ax+b) mod p$ nad konečným telesom GF(p)

- popíšte základné pojmy: konečné teleso, eliptická krivka nad konečným telesom, operácie definované nad EC.

- vytvorte program na sčítanie dvoch bodov na EC nad telesom GF(p)

Vstup: parametre krivky, body *P, Q* z danej krivky

Výstup: súčet *P+Q*

Vstupné parametre napr.:

$p = 2^{224}-1025$ alebo

p = 627710173538668076383578942320766641608390870039032496127 9

a = -3;

b=24551555460089438177402939151974517847691080581611912380 65;

xp=60204628237568865675821348058752611191669897663688468 4818;

yp=17405033229362203140485755228021941036402348892738665 0641;

Vstupné parametre napr.:

p = 2^{160}-2933

a=26030455878249847893794757688453278272165032252 8

b=17353637252166565262529838458968852181443354835 2

xp=12741043688184503698053390568221893863136302303 79

yp=57221905858043839003353999120142654787428655216 6

Vstupné parametre napr.:

p=2^224-1025

a=12404576574124969701442337182895859753361802999610504592418729761688

b=97035800620171133954831186027491806135168942819533785924565869910 02

xp=24976530810051270927037584984009121071093885269663350011731968108524

yp=84130267739323594344612082059586609672896599366392331321934278281 13

Vstupné parametre:

https://en.wikipedia.org/wiki/Elliptic_curve_cryptography

http://www.secg.org/sec2-v2.pdf

Zadanie 2.

Výpočet dvojnásobku bodu na eliptickej krivke (EC) $y^2 mod p = (x^3+ax+b) mod p$ nad konečným telesom GF(p)

- popíšte základné pojmy: konečné teleso, eliptická krivka nad konečným telesom,

operácie definované nad EC.

- vytvorte program na výpočet dvojnásobku bodu na EC nad telesom GF(p)

Vstup: parametre krivky, bod P z danej krivky

Výstup: 2-násobok bodu P

Zadanie 3.

Prevod čísla z dekadickej sústavy (DS) do zvyškovej číselnej sústavy (ZČS) a jeho spätný prevod zo ZČS do DS pomocou Čínskej vety o zvyškoch.

- Popíšte základný postup pri prechode z DS do ZČS a zo ZČS do DS

Vstup: číslo z DS, bázový vektor

Výstup: číslo zo ZČS

https://en.wikipedia.org/wiki/List_of_prime_numbers

Zadanie 4.

Overte, že pre vhodne zvolené parametre algoritmu RSA a náhodne zvolenú správu M dostanete šifrovaním a následným dešifrovaním správu M´, pričom platí M=M´.

- Popíšte postup pri šifrovaní a dešifrovaní v algoritme RSA.

Vstup: prvočísla p,q, číslo e, otvorený text M

Výstup: verejný kľúč, súkromný kľúč, zašifrovaný text C, M´

Zadanie 5.

Overte, že tajné kľúče vygenerované účastníkmi A a B v algoritme na výmenu kľúčov Diffie-Hellman sú rovnaké.

- Popíšte postup pri generovaní tajného kľúča *k*.

Vstup: prvočíslo *q*, primitívny koreň *a*, parametre kľúča X_A, X_B

Výstup: tajný kľúč *k*, parametre kľúča Y_A, Y_B

Zadanie 6.

Overte, že pre vhodne zvolené parametre algoritmu El Gamal a náhodne zvolenú správu M dostanete šifrovaním a následným dešifrovaním správu M´, pričom platí M=M´.

- Popíšte postup pri šifrovaní a dešifrovaní v algoritme El Gamal.

Vstup: prvočíslo *p*, náhodné čísla *q, x, k*

Výstup: verejný kľúč, súkromný kľúč, zašifrovaný text

Zadanie 7.

Pre dostatočne veľké číslo *n* otestujte Rabin-Millerovým testom, či je číslo *n* prvočíslo alebo zložené číslo.

- Popíšte postup pri testovaní prvočíselnosti.

Vstup: prirodzené číslo n

Výstup: 1, ak číslo je prvočíslo alebo 0, ak číslo je zložené číslo

Názov	Študenti
1. Sčítanie rozdielnych bodov na EC	
2. Sčítanie rovnakých bodov na EC	
3. Čínska veta o zvyškoch	
4. Šifrovanie, dešifrovanie RSA	
5. Generovanie kľúča Diffie-Hellman	
6. Šifrovanie, dešifrovanie El Gamal	
7. Rabin-Millerov test	