1. Utvorte vrstvenú sieť ku sieti X s tokom f (tok je vyznačený číslami v štvorci). Kapacita všetkých hrán je 1.

2. Vypočítajte hodnotu Jacobiho symbolov $\left(\frac{225}{37}\right)$, $\left(\frac{195}{833}\right)$.
3. Určte multiplikatívny rád čísla $2 \pmod{37}$.
4. Definujeme v Z_m logaritmus čísla n pri základe a takto

$$\log_a n = x \qquad \text{práve vtedy, keď} \qquad a^x = n.$$

   Vypočítajte $\log_2 15$ a $\log_2 17$ v Z_{37}.
5. Napíšte, čo je chromatický polynóm grafu. Napíšte tvar chromatického polynómu pre strom s V vrcholami.
6. RSA je šifrovací algoritmus pri ktorom $n = p.q$ (p, g sú prvočísla), e resp. d sú šifrovací resp. dešifrovací exponent. Parametre e, d sú volené tak, že

$$e.d \equiv 1 \pmod{\varphi(n)}, \qquad (1)$$

   kde $\varphi(n)$ je Eulerova funkcia vyjadrujúca počet prvkov menších ako n, ktoré sú s n nesúdeliteľné. Určte ľubovoľnú dvojicu e, d tak, aby vyhovovala danej podmienke (1), keď $p = 13, q = 17$. (Nepovinná časť: Ukážte, že pre $x \in Z_n, (x, n) = 1$ platí $D(E(x)) = (x^e)^d \equiv x \pmod{n}$.)
7. Napíšte maticu DFT pre 6 rozmerné vektory. Maticu napíšte pomocou $\omega = e^{2\pi i/6}$. Určte hodnoty, $\omega^j, j = 1, 2, 3, 4, 5, 6$.
8. Vypočítajte inverznú DFT pre vektor

$$(6; 1 + i; 0; 1 - i).$$

9. Vypočítajte pravdepodobnosť prenosu z najvyššieho bitu pri súčte dvoch náhodných n bitových slov.
10. Určte všetky nezávislé množiny pre graf G.

1000. Charakterizujte invertibilné prvky Z_m (t.j. určte, kedy je prvok $a \in Z_m$ invertibilný) a ukážte, že invertibilná prvky v Z_m tvoria grupu.

1. Utvorte vrstvenú sieť ku sieti X s tokom f (tok je vyznačený číslami v štvorci). Kapacita všetkých hrán je 1.

2. Vypočítajte hodnotu Jacobiho symbolov $\left(\frac{595}{207}\right)$, $\left(\frac{289}{43}\right)$.
3. Určte multiplikatívny rád čísla $2 \pmod{29}$.
4. Definujeme v Z_m logaritmus čísla n pri základe a takto

$$\log_a n = x \qquad \text{práve vtedy, keď} \qquad a^x = n.$$

   Vypočítajte $\log_2 7$ a $\log_2 8$ v Z_{29}.
5. Napíšte, čo je chromatický polynóm grafu. Napíšte tvar chromatického polynómu pre strom s V vrcholami.
6. RSA je šifrovací algoritmus pri ktorom $n = p.q$ (p, g sú prvočísla), e resp. d sú šifrovací resp. dešifrovací exponent. Parametre e, d sú volené tak, že

$$e.d \equiv 1 \pmod{\varphi(n)}, \qquad (1)$$

   kde $\varphi(n)$ je Eulerova funkcia vyjadrujúca počet prvkov menších ako n, ktoré sú s n nesúdeliteľné. Určte ľubovoľnú dvojicu e, d tak, aby vyhovovala danej podmienke (1), keď $p = 13, q = 19$. (Nepovinná časť: Ukážte, že pre $x \in Z_n, (x, n) = 1$ platí $D(E(x)) = (x^e)^d \equiv x \pmod{n}$.)
7. Napíšte maticu DFT pre 6 rozmerné vektory. Maticu napíšte pomocou $\omega = e^{2\pi i/6}$. Určte hodnoty, $\omega^j, j = 1, 2, 3, 4, 5, 6$.
8. Vypočítajte inverznú DFT pre vektor

$$(6; -1 - i; 0; i - 1).$$

9. Vypočítajte pravdepodobnosť prenosu z najvyššieho bitu pri súčte dvoch náhodných n bitových slov.
10. Určte všetky nezávislé množiny pre graf G.

1000. Charakterizujte invertibilné prvky Z_m (t.j. určte, kedy je prvok $a \in Z_m$ invertibilný) a ukážte, že invertibilná prvky v Z_m tvoria grupu.

1. Určte všetky nezávislé množiny pre graf G.

   6 bodov

2. a.) Overte či 2 je primitívny element Z_{37}^*.
   b.) Vypočítajte $\log_2 13$.

   10 bodov

3. Vyberte šifrovací a dešifrovací exponent pre $\mathrm{RSA}_{7.13}$, t.j. $n = 7.13 = 91$. Potom zašifrujte správu $x = 2$. Výsledok dešifrujte.

   10 bodov

4. Vypočítajte hodnotu Jacobiho symbolov $\left(\frac{105}{495}\right)$, $\left(\frac{105}{113}\right)$.

   6 bodov

5. Utvorte vrstvenú sieť ku sieti X s tokom f (tok je vyznačený číslami v štvorci). Kapacita všetkých hrán je 1.

   6 bodov

6. Nájdite blokovací tok siete algoritmom MPM (prípadne aj inou metódou).

   6 bodov

7. a.) Napíšte maticu DFT (diskrétnej Fourierovej transformácie) pre $n = 6$.
   b.) Vypočítajte $\mathrm{DFT}(1, 2, i, -i)$.

   10 bodov

8. a.) Uvažujme neorientované grafy na množine vrcholov $\{1, 2, 3, \ldots, 9, 10\}$. Pre akú časť z nich je $\{1, 2, 3, 4, 5\}$ nezávislá množina.
   b.) Napíšte, čo je to rez v sieti, kapacita rezu a napíšte vzťah medzi kapacitou rezu a tokom v sieti.

   6 bodov

1. Určte všetky nezávislé množiny pre graf G.

   6 bodov

2. a.) Overte či 7 je primitívny element Z_{41}^*.
   b.) Vypočítajte $\log_7 17$.

   10 bodov

3. Vyberte šifrovací a dešifrovací exponent pre $\mathrm{RSA}_{7.13}$, t.j. $n = 7.13 = 91$. Potom zašifrujte správu $x = 2$. Výsledok dešifrujte.

   10 bodov

4. Vypočítajte hodnotu Jacobiho symbolov $\left(\frac{723}{933}\right)$, $\left(\frac{105}{127}\right)$.

   6 bodov

5. Utvorte vrstvenú sieť ku sieti X s tokom f (tok je vyznačený číslami v štvorci). Kapacita všetkých hrán je 1.

   6 bodov

6. Nájdite blokovací tok siete algoritmom MPM (prípadne aj inou metódou).

   6 bodov

7. a.) Napíšte maticu DFT (diskrétnej Fourierovej transformácie) pre $n = 6$.
   b.) Vypočítajte $\mathrm{DFT}(2, 1, -i, i)$.

   10 bodov

8. a.) Uvažujme neorientované grafy na množine vrcholov $\{1, 2, 3, \ldots, 9, 10\}$. Pre akú časť z nich je $\{1, 2, 3, 4, 5\}$ nezávislá množina.
   b.) Napíšte, čo je to rez v sieti, kapacita rezu a napíšte vzťah medzi kapacitou rezu a tokom v sieti.

   6 bodov

1., 8 b Nájdite maximálny tok v sieti metódou vrstvených sietí (číslo v štvorci označuje tok, bez štvorca kapacitu):

2., 6 b Vypočítajte hodnotu Jacobiho symbolov $\left(\frac{280}{131}\right)$, $\left(\frac{280}{531}\right)$.

3., 8 b Pre metódu RSA_{77}, t.j. $n = 77$, zvolte vhodný šifrovací a dešifrovací exponent a zašifrujte správu $x = 13$ a následne dešifrujte .

4., 8 b Nájdite primitívny element α v Z_{17} a vypočítajte $\log_\alpha 7$ a $\log_\alpha 9$.

5., 8 b Nájdite všetky nezávislé množiny grafu

6., 8 b Nech $x \equiv 2 \pmod 3$,$x \equiv 3 \pmod 5$ a $x \equiv 6 \pmod 7$. Nájdite x také, že $x \equiv a_i \pmod{105}$ pre $i = 1, 2, 3$.

7., 6 b Nájdite riešenie rovnice $35x \equiv 14 \pmod{49}$.

8., 8 b Napíšte tabuľku logaritmov pri základe α (môžete zvoliť rovnaké, ako v príklade 4) v Z_{17}^*. Potom zvolte tajný parameter Boba $a, a \neq 1$ v El Gamalovom kryptosystéme, vypočítajte $\beta = \alpha^a \pmod{17}$. Odošlite Bobovi správu $x = 8$ a dešifrujte prijatú správu.

1000., 5 b Charakterizujte invertibilné prvky Z_m (t.j. určte, kedy je prvok $a \in Z_m$ invertibilný) a ukážte, že invertibilné prvky v Z_m tvoria grupu.

1., 8 b Nájdite maximálny tok v sieti metódou vrstvených sietí (číslo v štvorci označuje tok, bez štvorca kapacitu):

2., 6 b Vypočítajte hodnotu Jacobiho symbolov $\left(\frac{651}{791}\right)$, $\left(\frac{650}{791}\right)$.

3., 8 b Pre metódu RSA_{77}, t.j. $n = 77$, zvolte vhodný šifrovací a dešifrovací exponent a zašifrujte správu $x = 5$ a následne dešifrujte .

4., 8 b Nájdite primitívny element α v Z_{19} a vypočítajte $\log_\alpha 7$ a $\log_\alpha 9$.

5., 8 b Nájdite všetky nezávislé množiny grafu

6., 8 b Nech $x \equiv 3 \pmod 3$,$x \equiv 4 \pmod 5$ a $x \equiv 5 \pmod 7$. Nájdite x také, že $x \equiv a_i \pmod{105}$ pre $i = 1, 2, 3$.

7., 6 b Nájdite riešenie rovnice $33x \equiv 44 \pmod{77}$.

8., 8 b Popíšte ElGamalov kryptosystém. Potom napíšte tabuľku logaritmov pri základe α (môžete zvoliť rovnaké, ako v príklade 4) v Z_{19}^*. Ďalej zvolte tajný parameter Boba $a, a \neq 1$ v El Gamalovom kryptosystéme, vypočítajte $\beta = \alpha^a \pmod{19}$. Odošlite Bobovi správu $x = 5$ a dešifrujte prijatú správu.

1000., 5 b Charakterizujte invertibilné prvky Z_m (t.j. určte, kedy je prvok $a \in Z_m$ invertibilný) a ukážte, že invertibilné prvky v Z_m tvoria grupu.

1., 8 b Nájdite maximálny tok v sieti metódou vrstvených sietí (číslo v štvorci označuje tok, bez štvorca kapacitu):

2., 6 b Vypočítajte hodnotu Jacobiho symbolov $\left(\frac{583}{737}\right)$, $\left(\frac{582}{737}\right)$.

3., 8 b Pre metódu RSA_{91}, t.j. $n = 91$, zvolte vhodný šifrovací a dešifrovací exponent a zašifrujte správu $x = 3$ a následne dešifrujte .

4., 8 b Nájdite primitívny element α v Z_{23} a vypočítajte $\log_\alpha 7$ a $\log_\alpha 9$.

5., 8 b Nájdite všetky nezávislé množiny grafu

6., 8 b Nech $x \equiv 5 \pmod 3$,$x \equiv 4 \pmod 5$ a $x \equiv 5 \pmod 7$. Nájdite x také, že $x \equiv a_i \pmod{105}$ pre $i = 1, 2, 3$.

7., 6 b Nájdite riešenie rovnice $20x \equiv 15 \pmod{55}$.

8., 8 b Napíšte tabuľku logaritmov pri základe α (môžete zvoliť rovnaké, ako v príklade 4) v Z_{23}^*. Potom zvolte tajný parameter Boba $a, a \neq 1$ v El Gamalovom kryptosystéme, vypočítajte $\beta = \alpha^a \pmod{23}$. Odošlite Bobovi správu $x = 2$ a dešifrujte prijatú správu.

1000., 5 b Charakterizujte invertibilné prvky Z_m (t.j. určte, kedy je prvok $a \in Z_m$ invertibilný) a ukážte, že invertibilné prvky v Z_m tvoria grupu.

A

1. Napíštete všeobecný vzorec pre prvky matice rýchlej Fourierovej transformácie. Vypočítajte inverznú Fourierovu transfomáciu vektora: $(3; 2i; i; 1)$.

2. Vypočítajte hodnotu Jacobiho symbolov $\left(\frac{337}{533}\right), \left(\frac{329}{833}\right)$.

3. Pre metódu RSA_{143}, t.j. $n = 133 = 13.11$, zvolte vhodný šifrovací a dešifrovací exponent a zašifrujte správu $x = 2$. Následne dešifrujte.

4. Nájdite primitívny element α v Z_{17} a vypočítajte $\log_\alpha 7$ a $\log_\alpha 11$.

5. Metódou spätného prhľadávania nájdite všetky nezávislé množiny grafu

6. Zistite, či uvedená rovnica má riešenie. Pokiaľ áno, nájdite ho.

$$13x \equiv 21 \pmod{37}.$$

7. Určte vrstvenú sieť, pre sieť nižšie. Kapacita všetkých hrán je 1. Uvedené čísla ukazujú tok. V ostatných hranách je tok 0.

8. Napíšte, čo je chromatický polynóm grafu. Napíšte tvar chromatického polyncmu pre strom s V vrcholami.

A

1. Napíštete všeobecný vzorec pre prvky matice inverznej rýchlej Fourierovej transformácie. Vypočítajte inverznú Fourierovu transfomáciu vektora: $(1; 2i; 3; 4i)$.

2. Určte multiplikatívny rád čísla α modulo n ($\mathrm{ord}_n(\alpha) = \min\{i | i \in N^+, \alpha^i = 1 \pmod n\}$)

$$2 \pmod{15},$$

$$5 \pmod{17}.$$

3. Vypočítajte hodnotu Jacobiho symbolov $\left(\frac{564}{657}\right), \left(\frac{323}{427}\right)$.

4. Pre metódu RSA_{133}, t.j. $n = 133 = 7.19$, zvolte vhodný šifrovací a dešifrovací exponent a zašifrujte správu $x = 2$. Následne dešifrujte.

5. Nájdite primitívny element α v Z_{19} a vypočítajte $\log_\alpha 9$ a $\log_\alpha 15$.

6. Charakterizujte invertibilné prvky Z_m (t.j. určte, kedy je prvok $a \in Z_m$ invertibilný, dokážte). Určte počet invertibilných prvkov Z_{2332}.

7. Metódou spätného prhľadávania nájdite všetky nezávislé množiny grafu

8. Určte vrstvenú sieť, pre sieť nižšie. Kapacita všetkých hrán je 1. Uvedené čísla ukazujú tok. V ostatných hranách je tok 0.

B

1. Napíštete všeobecný vzorec pre prvky matice rýchlej Fourierovej transformácie. Vypočítajte Fourierovu transfomáciu vektora: $(i; 2; 3i; 4)$.

2. Určte multiplikatívny rád čísla α modulo n ($\mathrm{ord}_n(\alpha) = \min\{i | i \in N^+, \alpha^i = 1 \pmod{n}\}$)

$$7 \pmod{15},$$

$$2 \pmod{17}.$$

3. Vypočítajte hodnotu Jacobiho symbolov $\left(\frac{456}{567}\right), \left(\frac{317}{417}\right)$.

4. Pre metódu RSA_{143}, t.j. $n = 143 = 11.13$, zvolte vhodný šifrovací a dešifrovací exponent a zašifrujte správu $x = 2$. Následne dešifrujte.

5. Nájdite primitívny element α v Z_{17} a vypočítajte $\log_\alpha 9$ a $\log_\alpha 13$.

6. Charakterizujte invertibilné prvky Z_m (t.j. určte, kedy je prvok $a \in Z_m$ invertibilný, dokážte). Určte počet invertibilných prvkov Z_{1897}.

7. Metódou spätného prhľadávania nájdite všetky nezávislé množiny grafu

8. Určte vrstvenú sieť, pre sieť nižšie. Kapacita všetkých hrán je 1. Uvedené čísla ukazujú tok. V ostatných hranách je tok 0.