Inlämningsuppgift 1

Upgiften är individuell. Det är tillåtet att diskutera med kurskamrater, dock inte att plagiera. Du kan också använda lämpliga digitala verktyg så som miniräknare, dator program, osv. Du behöver däremot beskriva vad du har använt.

1. Kryptera texten "**Number theory and Cryptography is useful.**" med *Vigenèrechiffer* (enligt tabula recta med engelskt alfabet) med nyckeln (signaturen) FERMAT. (3p)

2. Kryptera samma text som uppgiften (1), samt en egen vald text (av ca. 35 tecken) med ett *kolumntranspositionskrypto*. Välj själv en nyckel med längd åtta. (3p)

3. Använd Vernamchiffret med en nyckelföljd 011011011011011... för att kryptera meddelandet MÖT MIG I KVÄLL, där alfabetet kodas som 'A '=00000 (0), 'B'=00001 (1), 'C'=00010 (2), 'D'=00011 (3), ... 'Ö'=11100 (28), ' ' = 11101 (29), '1'=11110 (30), '2'=11111 (31). Ge kryptotexten uttryckt i bokstäver. ('1' och '2' är med som utfyllnad.) (3p)

4. Du har fått ett krypterat meddelande, `ARU-KY-REDRCRTGL-AÄKOURHN-T-TA-KTP-` och misstänker att det är krypterat med ett kolumntranspositionskrypto. Vi kan misstänka att texten fyller upp en kolumntranspositionstabell med ett visst antal rader och kolumner. Vad finns det då för möjliga antal kolumner? Försök dekryptera. (3p)

5. Låt A, B och C vara tre icke-tomma mängder. Är följande påstående sant eller falskt? Om det är sant, så motivera varför. Om det är falskt, så ge ett motexempel. (3p)

   (a) Om $A \cap B = A \cap C$, så gäller $B = C$.

   (b) Om $A \cup B = A \cup C$, så gäller $B = C$.

   (c) $(A \setminus B) \cap (A \setminus C) = A \setminus (B \cup C)$.

   $\mathbb{N}$ betecknar mängden av alla naturliga tal och $\mathbb{Z}$ betecknar mängden av alla heltal.

6. Ge exempel på oändliga mängder A, B och C som uppfyller följnade villkor: (3p)

   - Var och en av mängderna är delmängder av $\mathbb{N}$.
   - $A \cap B \cap C = \emptyset$,
   - Varje snitt mellan två av mängderna inte är tomt.

   Presentera också ditt svar med hjälp av Venn-diagram.

7. Låt $5\mathbb{N} = \{5n : n \in \mathbb{N}\} = \{0, 5, 10, 15, \dots\}$ och $4\mathbb{N} = \{4n : n \in \mathbb{N}\} = \{0, 4, 8, 12, \dots\}$. (3p)

   - Beskriv mängderna $5\mathbb{N} \cup 4\mathbb{N}$ och $5\mathbb{N} \cap 4\mathbb{N}$ (på lämpligt sätt).
   - Finns det ett tal k så att $5\mathbb{N} \cup 4\mathbb{N} = k\mathbb{N}$?
   - Finns det ett tal k så att $5\mathbb{N} \cap 4\mathbb{N} = k\mathbb{N}$?

8. Kursen Talteori och kryptografi går så väl på distans som på campus. Dessutom går kursen som en obligatorisk programkurs samt en fristående kurs. I år finns 113 distans och 157 campus studenter registrerade på kursen. Det fanns 35 program studenter som läser kursen på distans, och 48 fristående studenter som läser kursen på campus. En student får inte registrera sig till kursen både som campus och distans; samt både som program och fristående. Hur många program respektive fristående studenter läser kursen? (3p)

9. På en mindre danstillsättning för vals och salsa befinner sig fyra kvinnor $K = \{$Viktoria, Anna, Lisa, Sanna$\}$ och tre män $M = \{$ Fredrik, Ola, Adam $\}$. (3p)

   - Hur kan mängden av möjliga danspar (där samma par med olika danser räknas endast en gång) beskrivas som produktmängden och hur stor blir denna mängd?
   - Tyvärr dansar Viktoria och Anna endast vals och Fredrik och Adam endast salsa. Ange delmängden av möjliga danspar och dess kardnalitet (där samma par med olika danser räknas flera gånger).

10. En försäljare sålde ett antal falskor blåbärssaft på RIKO-Ring Skövde. Försäljaren hade små flaskor (0,5 liter) som kostade 19 kr och stora flaskor (2 liter) som kostade 69 kr. När dagen slutade hade försäljaren sålt 93 flaskor och fått 4567 kr. Hur många liter saft hade hen sålt? (3p)

11. Ge exempel på funktioner som uppfyller följande: (3p)

    (a) En bijektiv funktion $b : \mathbb{N} \to 2\mathbb{N}$.

    (b) En funktion $g : \mathbb{N} \to \mathbb{N}$ som är injektiv men inte surjektiv

    (c) En funktion $h : \mathbb{N} \to \mathbb{N}$ som är surjektiv men inte injektiv.

12. Beskriv en funktion $f : \mathbb{Z} \to \mathbb{N}$ som är bijektiv.[1] Bestäm också funktionens invers $f^{-1}(x)$. (3p)

[1] Tips: Behandla negativa och positiva tal olika som argument, och jämför med föregående.