Provkonstruktion

Årskurs: Gymnasiet

Kurs: Matematik 3b

Tema: Talteori och kryptografi

Syfte

Syftet med provet är att bedöma elevernas förståelse och tillämpning av begreppet talteori, med särskilt fokus på primtal och deras betydelse inom kryptografi. Provets frågor avser att mäta elevernas kunskaper om primtalens egenskaper, kryptografiska algoritmer och deras tillämpningar i samhället.

Koppling till styrdokument

Centralt innehåll

Denna lektion syftar till att introducera begreppet talteori, med fokus på primtal och deras betydelse inom kryptografi. Eleverna kommer att lära sig om egenskaper hos primtal, hur de används inom säkerhetsprotokoll och grundläggande kryptografiska metoder, inklusive RSA-algoritmen.

Kunskapskrav

Eleven ska kunna redogöra för och tillämpa grundläggande begrepp inom talteori, inklusive primtal och deras egenskaper. Dessutom ska eleven kunna förklara hur dessa koncept används inom kryptografi.

Prov

Faktafrågor

1. Vilket av följande är ett primtal?

A. 1

B. 4

C. 6

D. **7**

2. Vilket av följande tal är inte ett primtal?

A. 13

B. 17

C. **21**

D. 23

3. Vad står RSA för i kryptografi?

A. Random Secure Algorithm

B. **Rivest Shamir Adleman**

C. Rapid Security Analysis

D. Robust Security Algorithm

4. Vilket tal är endast delbart med 1 och sig självt?

A. **5**

B. 9

C. 10

D. 15

5. Vilken metod används för att identifiera primtal?

A. Sieve of Newton

B. **Sieve of Eratosthenes**

C. Factorization Method

D. Cryptographic Validation

6. Vad är en egenskap hos primtal?

A. De har oändligt många delare.

B. **De kan endast delas jämnt med 1 och sig själva.**

C. De är alltid jämna tal.

D. De är alltid större än 10.

7. Vad används primtal för inom kryptografi?

A. Återställning av lösenord

B. **Kryptering av data**

C. Tidsberäkning

D. Ingenjörsberäkningar

8. Vad är ett sammansatt tal?

A. **Ett tal större än 1 som inte är ett primtal.**

B. Ett tal som endast är delbart med 1 och sig självt.

C. Ett negativt heltal.

D. Ett heltal som är jämnt.

9. I RSA-algoritmen används vilka typer av tal för nyckelgenerering?

A. Endast negativa tal.

B. **Primtal.**

C. Sammansatta tal.

D. Udda tal.

10. Vilken är en tillämpning av kryptografi i vardagen?

A. Energihushållning

B. **Banktransaktioner**

C. Sportanalys

D. Djurhållning

11. Vad behövs för att utföra ett primtalstest?

A. Regelbundenhet

B. **En algoritm och ett heltal.**

C. Datorprogram

D. Matematiska formler

12. Vad är syftet med kryptografi?

A. Att dela ut information offentligt.

B. **Att skydda information från obehörig åtkomst.**

C. Att förlora data.

D. Att öka hastigheten på elektroniska transaktioner.

13. Vad är nyckeln i kryptografi?

A. En typ av algorithm.

B. **Ett värde som används för kryptering och dekryptering av data.**

C. En säkerhetsåtgärd.

D. Ett dataformat.

14. Vilken typ av algoritm använder RSA?

A. Symmetrisk

B. **Asymmetrisk**

C. Hash-algoritm

D. Klassisk

15. Vad kännetecknar en kryptografisk metod?

A. Den är alltid öppen för alla.

B. **Den ska vara svår att bryta utan rätt nyckel.**

C. Den fungerar bara för låga tal.

D. Den baseras på sammansatta tal.

Resonerande frågor

1. Diskutera hur primtal kan påverka cybersäkerheten. Förklara varför dessa tal är centrala.

Syftet med frågeställningen är att ge eleverna möjlighet att koppla teorin om primtal till praktiska tillämpningar i cybersäkerhet.

2. Vilka begränsningar ser du med att använda primtal i kryptografi, och hur

kan dessa övervinnas?

Denna fråga uppmuntrar eleverna att tänka kritiskt på utmaningar inom kryptografi och presentera argument och möjliga lösningar.

3. Hur kan talteori appliceras inom andra områden av matematik eller datavetenskap än kryptering?

Här får eleverna möjlighet att visa sin förmåga att koppla samman kunskap från olika ämnesområden.

4. Förklara vikten av primtal i skapandet av säkra kommunikationssystem. Ge specifika exempel.

Frågan uppmuntrar komplexa resonemang och exemplifieringar kring praktiska tillämpningar av primtal.

5. Argumentera för varför RSA-algoritmen är eller inte är säker i dagens digitala samhälle.

Eleverna ges chans att använda kritiskt tänkande för att utvärdera moderna kryptografiska metoder.

6. Beskriv hur talteori kan förändra vår förståelse av algoritmer över tid.

Genom att reflektera över historiska och framtida tillämpningar ges eleverna möjlighet att bredda sina perspektiv.

7. Diskutera hur kryptografi har påverkat utvecklingen av internet och datakommunikation.

Denna fråga uppmanar till att analysera det bredare sammanhanget av kryptografi och dess roll i samhälle och teknik.

8. Hur kan utbildning i talteori förbättra programmering och algorithm design?

Genom att koppla matematiska koncept till praktiska färdigheter i programmering ges eleverna möjlighet att se värdet av sin matematikutbildning.

Bedömning

Provets faktadel består av 15 frågor, där varje fråga ger 1 poäng. De resonerande frågorna ger upp till 3 poäng vardera. För betygsnivå E krävs minst 8 poäng, för betygsnivå C minst 12 poäng (varav minst 3 poäng från resonerande frågor) och för betygsnivå A minst 18 poäng (varav minst 5

poäng från resonerande frågor).

Tags: Prov