Lösningar till tenta D1401 4, 2025-03-27

1. (a) $\sqrt{2365} = 48.63\ldots$ lista primtalen ≤ 47 för Eratosthenes:

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47

2357 ej jämnt delbart med något av dessa så <u>primtal</u>

$2359 = 7 \cdot 337$ så <u>sammansatt</u>

$2361 = 3 \cdot 787$ så <u>sammansatt</u>

$2363 = 17 \cdot 139$ så <u>sammansatt</u>

$2365 = 5 \cdot 473$ så <u>sammansatt</u>

(b) Alltså är $p = 2357$ och vi ska beräkna $\gcd(12421, 2356)$

$$12\,421 = 5 \cdot 2356 + 641$$
$$2356 = 3 \cdot 641 + 433$$
$$641 = 1 \cdot 433 + 208$$
$$433 = 2 \cdot 208 + 17$$
$$208 = 12 \cdot 17 + 4$$
$$17 = 4 \cdot 4 + 1$$

så $\gcd(12421, 2356) = \underline{\underline{1}}$

(c) Eftersom 12421 och 2356 är rel. prima kan Eulers sats användas för att beräkna diskret exponentiering. Först primtalsfaktorisering av $2356 = 2^2 \cdot 19 \cdot 31$ så $\phi(2356) = 2^1 \cdot (2-1)(19-1)(31-1) = 1080$

och $42124 \equiv 42124 - 39 \cdot 1080 = 4 \pmod{1080}$

så $\underbrace{12421}_{\equiv 641}{}^{42124} \equiv 641^4 \equiv (410\,881 - 174 \cdot 2356)^2 \equiv 937^2 \equiv$

$\equiv 877969 - 372 \cdot 2356 = \underline{\underline{1537}}$

(d) Fältet $\mathbb{F}_p$ innehåller p tal: $0, 1, \dots, p-1$. Av dessa är $\phi(p-1)$ generatorer. Om dessa fördelar sig jämnt över fältet är det

ung. $2\frac{\phi(p-1)}{3}$ generatorer som är $> \frac{p}{3}$

Eftersom $\phi(p-1) = \phi(2358) = 1080$ är det uppskattningsvis $2 \cdot \frac{1080}{3} = \underline{720}$ generatorer som är ≥ 786.

(Det verkliga antalet generatorer ≥ 786 är 735.)

---

2. <u>Monoalfabetiskt substitutionskrypto</u> (om man håller skivorna fixerade under kryptering) och <u>polyalfabetiskt substitutionskrypto</u> (om man skiftar krypteringsskivorna under krypteringsprocessen). Båda ger rätt svar.

3.
$$\underbrace{x^4-1}_{\equiv x^4+6} = (2x)(4x^3+5x+1) + 4x^2+5x+6$$

(senaste sida)

$$4x^3+5x+1 = (x+4)(4x^2+5x+6) + 5$$

$$\begin{aligned}
5 &= 4x^3+5x+1 - (x+4)(4x^2+5x+6) \\
&= 4x^3+5x+1 - (x+4)\left(x^4+6 - 2x(4x^3+5x+1)\right) \\
&= \left(1+(x+4)2x\right)(4x^3+5x+1) - (x+4)(x^4+6) \\
&\equiv (2x^2+x+1)(4x^3+5x+1) - (x+4)(x^4-1)
\end{aligned}$$

$$\begin{aligned}
1 \equiv 3 \cdot 5 &\equiv 3\left((2x^2+x+1)(4x^3+5x+1) - (x+4)(x^4-1)\right) \\
&\equiv (6x^2+3x+3)(4x^3+5x+1) - (3x+5)(x^4-1)
\end{aligned}$$

dvs $(4x^3+5x+1)^{-1} \bmod x^4-1 = \underline{6x^2+3x+3}$

$$4x^3+5x+1 \,\overline{)\, x^4+6}\quad 2x$$
$$-(x^4+3x^2+2x)$$
$$4x^2+5x+6$$

$$4x^2+5x+6 \,\overline{)\, 4x^3+5x+1}\quad x+4$$
$$-(4x^3+5x^2+6x)$$
$$2x^2+6x+1$$
$$-(2x^2+6x+3)$$
$$5$$

---

4. De övriga finalisterna var <u>Twofish</u>, <u>Serpent</u>, <u>MARS</u> och <u>RC6</u>.

---

5. <u>Bibelkoden</u>

---

6. <u>QKD</u> (Quantum Key Distribution)

---

7. (a) $n=77 \quad h(m)=26$

$=\underbrace{7}_{p}\cdot\underbrace{11}_{q}$ så $\phi(n)=(p-1)(q-1)=6\cdot 10=60$

a rel. prima med $60=2^2\cdot 3\cdot 5$ så minsta är $\underline{a=7}$

$\gcd(p-1,q-1)=\gcd(\underbrace{6}_{2\cdot 3},\underbrace{10}_{2\cdot 5})=2$ så

$$\text{lcm}(p-1,q-1)=\frac{(p-1)(q-1)}{\gcd(p-1,q-1)}=\frac{60}{2}=\underline{30}=b$$

$30=4\cdot 7+2 \qquad 1=7-3\cdot 2$

$7=3\cdot 2+1 \qquad\; =7-3(30-4\cdot 7)$

$\qquad\qquad\qquad\; =13\cdot 7-3\cdot 30$

så $d=a^{-1} \bmod b$

$=7^{-1} \bmod 30$

$=\underline{13}$

Signering: $s=26^7 \bmod 77\equiv$

$\equiv(26^3-228\cdot 77)(26^4-5934\cdot 77)=$

$\equiv 20\cdot 58-15\cdot 77=\underline{5}$

(b) $s^d \bmod n = 5^{13} \bmod 77 =$

$= 1\,220\,703\,125 - 15\,853\,287 \cdot 77$

$= 26$