

Vilket svar är rätt?

R: röd, G: grön, B: blå

1. Vad är $31^{38} \pmod{13}$?

R: 1, G: 7, B: 12

2. Vad är $53^{71} \pmod{35}$?

R: 1, G: 2, B: 34

3. Vad är d i ett RSA-system med $(n, e) = (143, 13)$?

R: 11, G: 37, B: 49

4. C har D_B och finner A:s $y = E_B(D_A(x))$ till B.

Kan C ändra i x och få B tro det kommer från A?

R: Ja, G: Nej, B: Kanske

5. Vad är $11^{12} + 13^{10} \pmod{143}$?

R: 1, G: 87, B: 120

6. Är 341 ett carmichaeltal?

R: Ja, G: Nej, B: Beror sig på

Svar:

1. B, ty $31^{38} \equiv_{13} 5^{38} \equiv_{13} (5^{12})^3 \cdot 5^2 \equiv_{13} 1^3 \cdot 25 \equiv_{13} 12$
($5^{12} \equiv_{13} 1$, 13 är ett primtal och $13 \nmid 5$ (Fermats lilla sats)).
2. G, ty $53^{71} = 18^{71}$ i $\mathbb{Z}_{35}$, $\text{sgd}(18, 35) = 1$ (så 18 är inverterbart i $\mathbb{Z}_{35}$) och
 $\phi(35) = \phi(5 \cdot 7) = 4 \cdot 6 = 24$, så (med Eulers sats)
 $18^{71} = (18^{24})^3 \cdot 18^{-1} = 1^3 \cdot 18^{-1} = 2$ (ty $18 \cdot 2 = 1$) i $\mathbb{Z}_{35}$.
3. G, ty $n = 143 = 11 \cdot 13$ ger (11 och 13 olika primtal) $m = 10 \cdot 12 = 120$.
 $120 = 13 \cdot 9 + 3$, $13 = 3 \cdot 4 + 1$ (så $\text{sgd}(13, 120) = 1$, $e = 13$ är möjligt och)
 $1 = 13 - 4 \cdot 3 = 13 - 4(120 - 9 \cdot 13) = -4 \cdot 120 + 37 \cdot 13$, så $d = 37$.
(Det räcker att $e \cdot d \equiv_{\text{mgm}(10,12)} 1$. Det ger $d = 37 + 60n$, $n \in \mathbb{N}$ möjliga.)
4. B/G, ty med D_B och (den allmänt kända) E_A får C fram (och kan ändra) x ,
men också D_A behövs för att skapa och skicka $E_B(D_A(x'))$.
5. R, ty (med Fermats lilla sats (11 och 13 är primtal, $10 = 11 - 1$, $12 = 13 - 1$))
 $11^{12} + 13^{10} \equiv_{11} 0^{12} + 1 = 1$ och $11^{12} + 13^{10} \equiv_{13} 1 + 0^{10} = 1$,
så ($143 = 11 \cdot 13$, $\text{sgd}(11, 13) = 1$) $11^{12} + 13^{10} \equiv_{143} 1$.
6. G, ty $341 = 11 \cdot 31$, 31 primtal och $(31 - 1) \nmid (341 - 1)$.