

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. A skickar x krypterat som $y = E_B(D_A(x))$ till B,
men råkar kasta x och spara y .
Hur återfår han x ?

R: Avkrypterar, G: Ger upp, B: Frågar B

5. Är 341 ett carmichaeltal?

R: Ja, G: Nej, B: Beror sig på

Svar:

1. B, ty $31^{38} \equiv_{13} 5^{38}$ och eftersom $13 \nmid 5$ och 13 är ett primtal fås (Fermat) att $5^{12} \equiv_{13} 1$ och således $5^{38} = (5^{12})^3 \cdot 5^2 \equiv_{13} 1^3 \cdot 5^2 = 25 \equiv_{13} 12$.
2. G, ty $53^{71} \equiv_{35} 18^{71}$ och eftersom $35 = 5 \cdot 7$ (5 och 7 primtal med $(5-1)(7-1) = 24$) är $18^{73} = 18^{3 \cdot 24 + 1} \equiv_{35} 18$, så $(\text{sgd}(18, 35) = 1$, så 18 inverterbart i $\mathbb{Z}_{35}$, $18^{-1} = 2$)
 $18^{71} = 18^{73} \cdot 18^{-2} \equiv_{35} 18 \cdot 18^{-2} = 18^{-1} \equiv_{35} 2$.
3. G, ty $n = 143 = 11 \cdot 13$ ger $m = (11-1)(13-1) = 120$.
 d ska uppfylla $e \cdot d \equiv_m 1$, dvs $13d \equiv_{120} 1$.
Euklides algoritm: $120 = 13 \cdot 9 + 3$, $13 = 3 \cdot 4 + 1$ ger
 $1 = 13 - 4(120 - 9 \cdot 13) = -4 \cdot 120 + 37 \cdot 13$ och vi kan ta $d = 37$.
4. B (eller G), ty han kan själv inte finna x utgående från y (och E_A , D_A och E_B).
5. G, ty $341 = 11 \cdot 31$ och $(31-1) \nmid (341-1)$
 $(3^{340} \equiv_{341} 56$, så 341 klarar inte fermatetestet med bas 3).