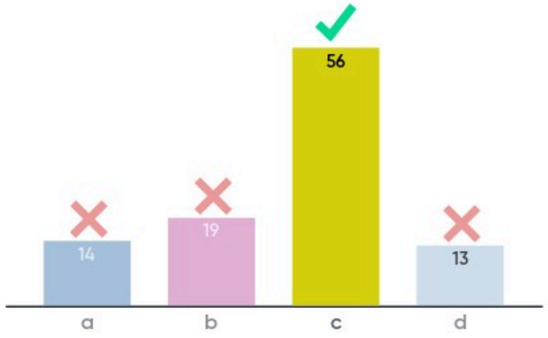
Fermats lille teorem sier

a) $a^{p-1} \equiv 0 \ (mod \ p)$ **b)** $a^{p} \equiv 1 \ (mod \ p-1)$

c) $a^{p-1} \equiv 1 \ (mod \ p)$ **d)** $a^{p} \equiv 1 \ (mod \ p)$



Join at menti.com use code 4387 6853

NTNU
Kunnskap for en bedre verden

Eulers teorem sier (for $a \perp m$):

0

a. $a^{\phi(m)} \equiv 1 \ (mod \ m)$

b. $a^{m} \equiv 1 \ (mod \ \phi(m))$

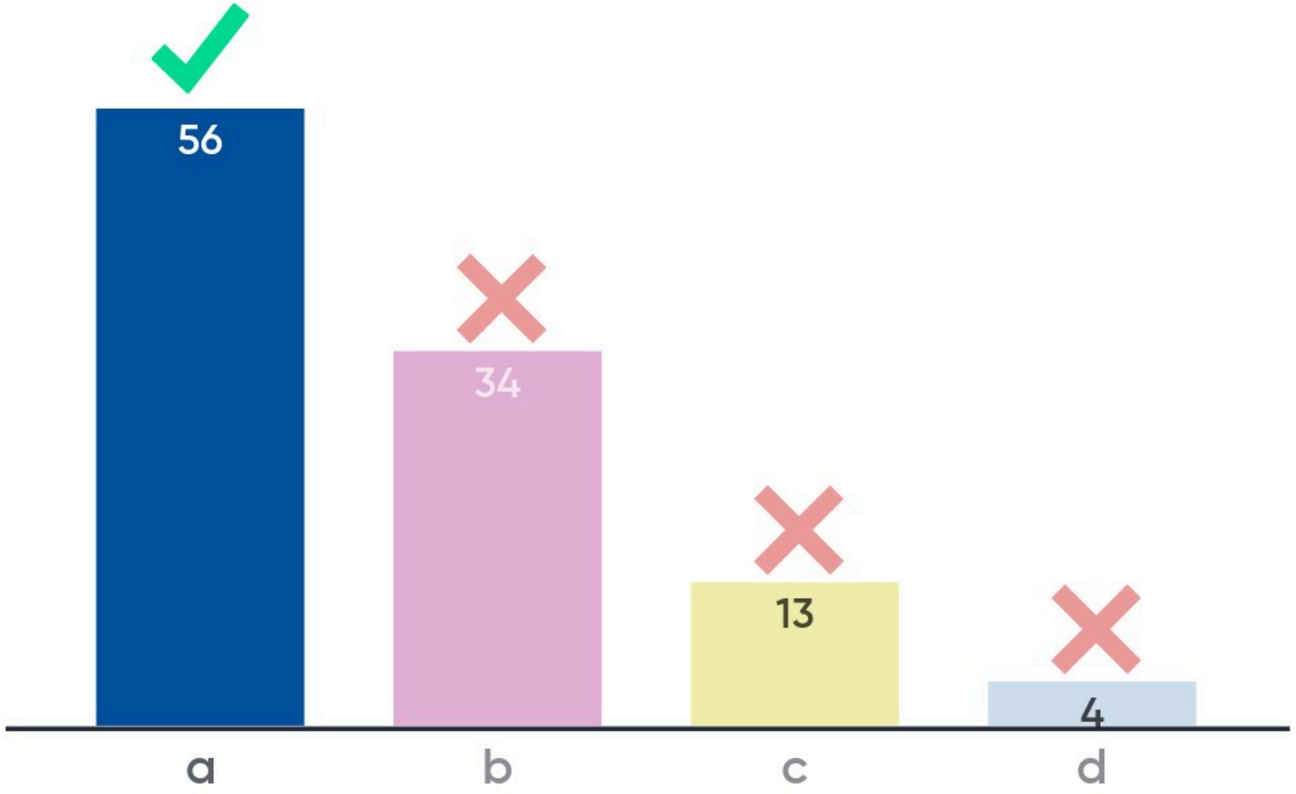
c. $a^{\phi(m)} \equiv 0 \ (mod \ m)$

d. $a^{m} \equiv 1 \ (mod \ m)$

0	0	0	0
a	b	c	d

00:03

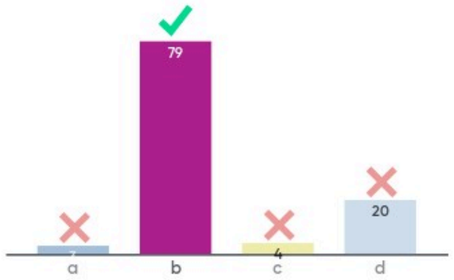
Eulers teorem sier (for $a \perp m$):



Hvis $N = p \cdot q$, så er $\phi(N) =$

a) p/q **b)** $(p-1)(q-1)$ **c)** $(p+q)/2$

d) $(p-1)(p-2)\ldots(p-q)$



Join at menti.com use code 3505 8070

NTNU
Kunnskap for en bedre verden

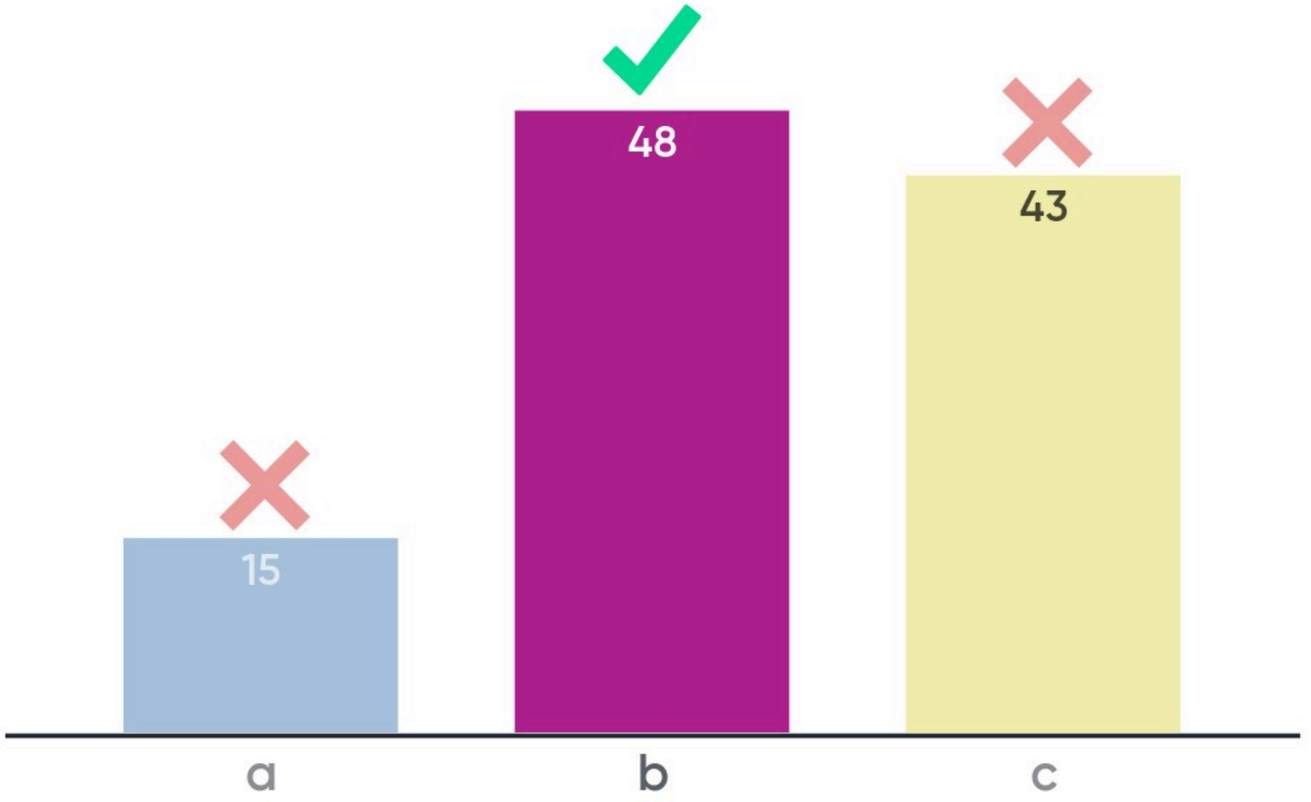
Hva er riktig?

0

a) Kryptologi er å lage koder, kryptografi er å knekke koder, og begge er kryptanalyse.
b) Kryptografi er å lage koder, kryptanalyse er å knekke koder, og begge er kryptologi.
c) Kryptologi er å lage koder, kryptanalyse er å knekke koder, og begge er kryptografi.

00:21

Hva er riktig?



Join at menti.com use code 8282 2918

NTNU
Kunnskap for en bedre verden

I Diffie–Hellman nøkkelutveksling så ender Alice og Bob opp med den delte nøkkelen:

0

a) $A + B = g^a + g^b$

b) $A \cdot B = g^{a+b}$

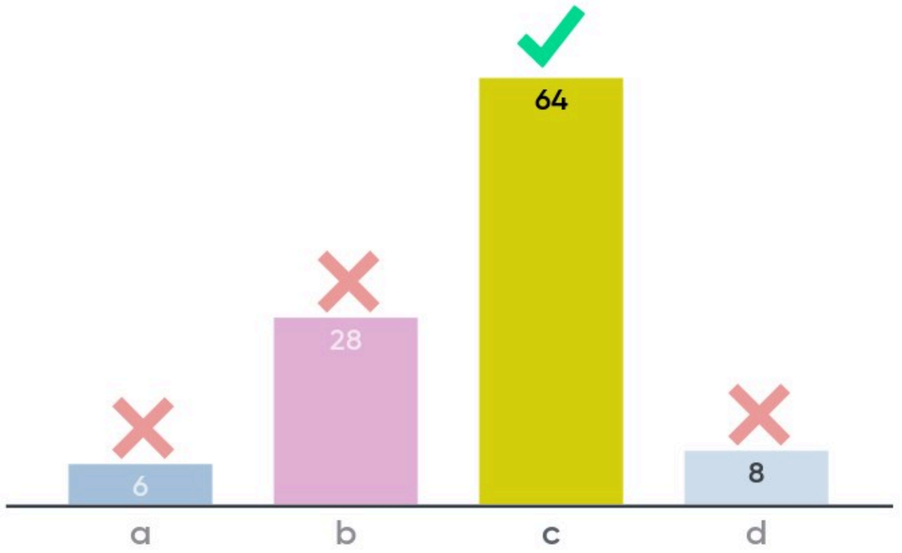
c) $A^b = B^a = g^{ab}$

d) $A^B = g^{ag^b}$

a b c d

00:13

I Diffie–Hellman nøkkelutveksling så ender Alice og Bob opp med den delte nøkkelen:



Join at **menti.com** use code **7753 3021**

NTNU
Kunnskap for en bedre verden

Finn en feil: Med offentlig nøkkel-kryptografi så ...

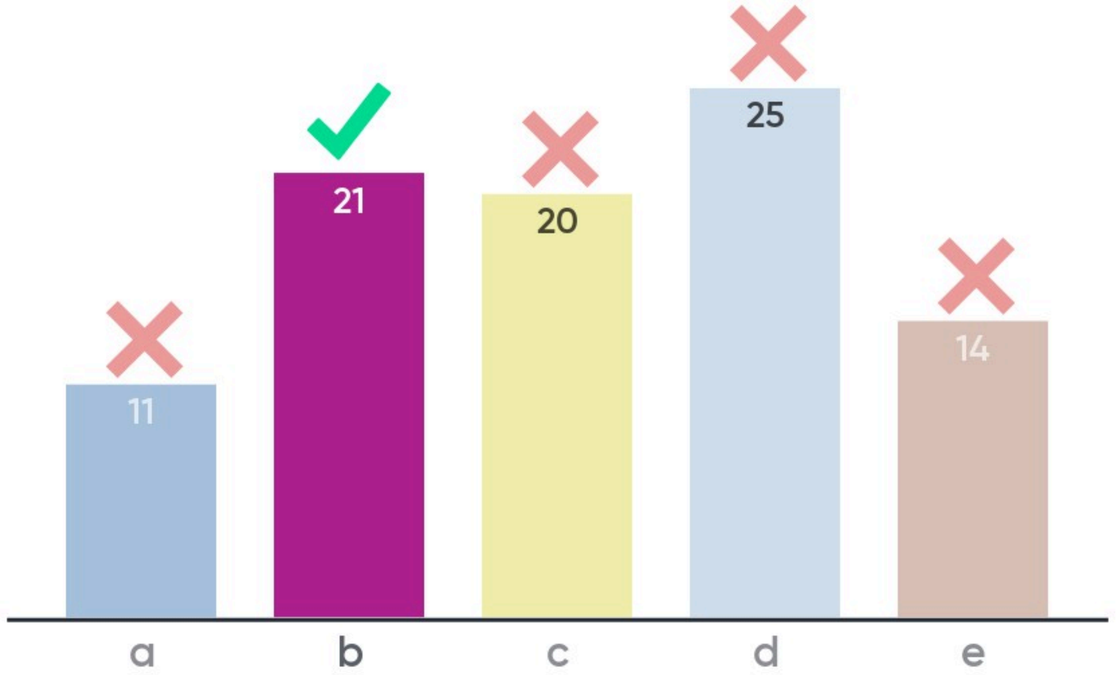
0

a) kan Bob dele den offentlige nøkkelen sin med hvem som helst.
b) kan Bob lese meldinger som Alice sender ham, så lenge Bob har den offentlige nøkkelen til Alice.
c) kan hvem som helst med den offentlige nøkkelen til Bob, sende en hemmelig melding til Bob.
d) kan hvem som helst med den offentlige nøkkelen til Bob, utføre nøkkelutveksling med Bob.
e) kan Bob digitalt signere dokumenter som hvem som helst kan verifisere.

0	0	0	0	0
a	b	c	d	e

00:13

Finn en feil: Med offentlig nøkkel-kryptografi så ...



Join at **menti.com** use code **1277 0439**

NTNU
Kunnskap for en bedre verden

Hvorfor kan ikke Eva knekke RSA-kryptering?

0

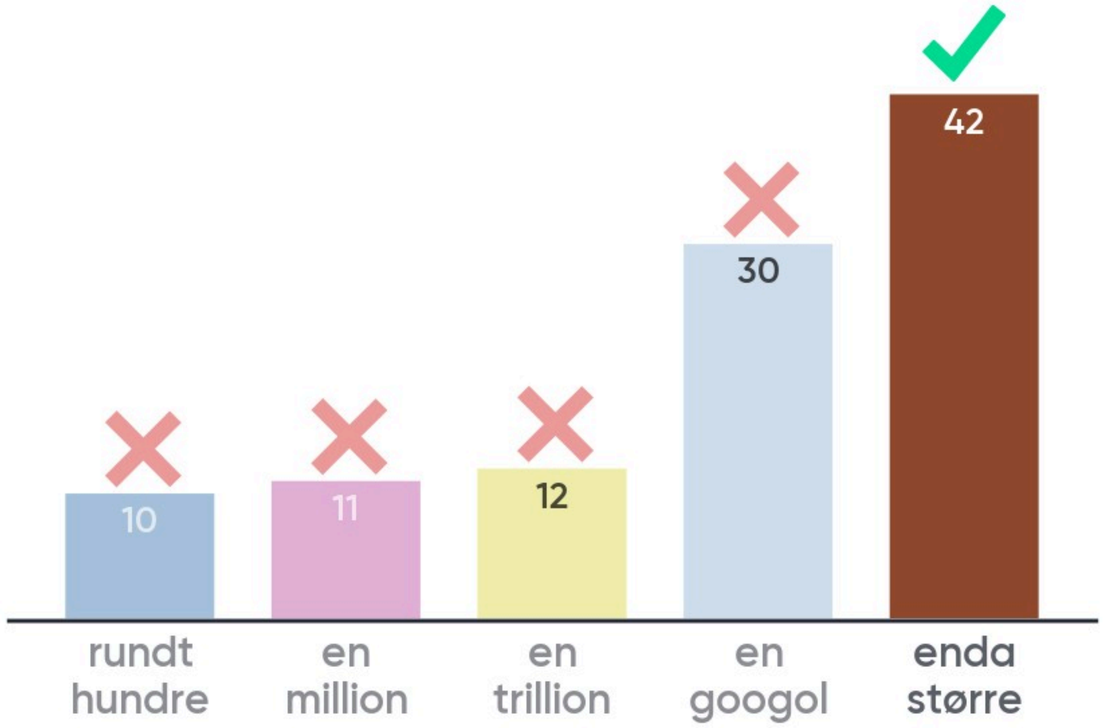
a) Fordi hun ikke husker formelen for $\phi(N)$.
b) Fordi hun trenger inversen til e, og hun kan ikke regne inverser.
c) Fordi hun trenger å faktorisere N for å regne ut $\phi(N)$, og hun kan ikke faktorisere.
d) Fordi hun trenger N for å regne ut $\phi(N)$, og N er hemmelig.

0	0	0	0
a	b	c	d

00:11

Hvorfor kan ikke Eva knekke RSA-kryptering?

Ca. hvor stor må N være for at RSA skal være sikkert?



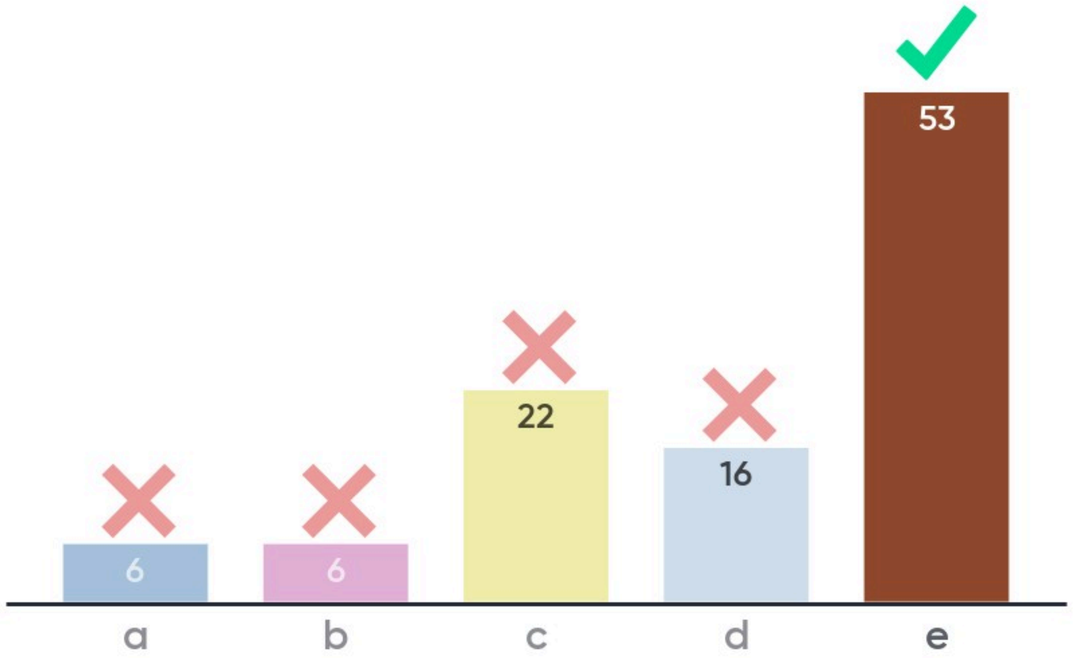
Join at menti.com use code 6590 8468

NTNU
Kunnskap for en bedre verden

Bonus: med en kvantedatamaskin kan man ...

0

a) Gjøre alt som en vanlig datamaskin kan, bare mer effektivt.
b) Simulere kvantefysikk effektivt.
c) Faktorisere tall effektivt.
d) Regne diskrete logaritmer effektivt.
e) Alle disse unntatt a).

00:14

Bonus: med en kvantedatamaskin kan man ...