Svar och anvisningar till de extra exemplen

Övning 10, on 11 oktober

1. RSA med $n = 77 = 7 \cdot 11$, så $m = (7-1)(11-1) = 60$.
a. $\text{sgd}(45, m) = 15 \neq 1$, så 45 duger inte som e.
b. Euklides algoritm ger $1 = -8 \cdot 60 + 37 \cdot 13$, så $d = 37$.
(Det räcker att $e \cdot d \equiv 1 \pmod{\text{mgm}(6, 10)}$, vilket ger det möjliga värdet $d = 7$.)
c. 3 krypteras som $E(3) \equiv 3^{13} \pmod{77}$. Man finner $(3^2 = 9, 3^4 = 81 \equiv 4, 3^8 \equiv 16)$ $3^{13} = 3^8 \cdot 3^4 \cdot 3 \equiv 16 \cdot 4 \cdot 3 \equiv 38 \pmod{77}$, så 3 krypteras som 38.
d. 2 avkrypteras som $D(2) \equiv 2^{37} \equiv 2^7 \pmod{77}$. Man finner $D(2) = 51$.

2. RSA med $n = 265 = 5 \cdot 53$, så $m = (5-1)(53-1) = 208$. $e = 37$ och Euklides algoritm ger $1 = -8 \cdot 208 + 45 \cdot 37$, så $d = 45$. Meddelandet 2 avkrypteras alltså som $D(2) \equiv 2^{45} \equiv 147 \pmod{265}$, så som 147.
($e \cdot d \equiv 1 \pmod{\text{mgm}(4, 52) = 52}$ ger här samma $d = 45$.)

3. $E(x) \equiv 718^e = 718^{143} \pmod{1333}$ och $e = 143 = (10001111)_2$.
$x^2 = 718^2 = 515524 \equiv 986 \pmod{1333}$, $x^4 = 986^2 = 972196 \equiv 439 \pmod{1333}$ etc. ger $E(x) \equiv x^{128} \cdot x^8 \cdot x^4 \cdot x^2 \cdot x \equiv 986 \cdot 769 \cdot 439 \cdot 986 \cdot 718 \equiv 707 \pmod{1333}$, så $E(718) = 707$.
Alternativt kan man räkna så (eftersom $143 = (10001111)_2$):
$E(x) \equiv (((((((1^2 \cdot \underset{1}{x})^2 \cdot \underset{0}{1})^2 \cdot \underset{0}{1})^2 \cdot \underset{0}{1})^2 \cdot \underset{1}{x})^2 \cdot \underset{1}{x})^2 \cdot \underset{1}{x})^2 \cdot \underset{1}{x} \pmod{1333}$.
P.s.s. fås $E(719) \equiv (((((((1^2 \cdot 719)^2 \cdot 1)^2 \cdot 1)^2 \cdot 1)^2 \cdot 719)^2 \cdot 719)^2 \cdot 719)^2 \cdot 719 \equiv \cdots \equiv 615 \pmod{1333}$ och $E(719) = 615$.
$n = 1333 = 31 \cdot 43$ ger $m = 30 \cdot 42 = 1260$.
Euklides algoritm: $1260 = 8 \cdot 143 + 116$, $143 = 1 \cdot 116 + 27$, $116 = 4 \cdot 27 + 8$, $27 = 3 \cdot 8 + 3$, $8 = 2 \cdot 3 + 2$, $3 = 1 \cdot 2 + 1$, så $1 = 3 - 2 = 3 - (8 - 2 \cdot 3) = -8 + 3 \cdot 3 = \cdots = -53 \cdot 1260 + 467 \cdot 143$, så vi tar $d = 467$.
(Här ger $e \cdot d \equiv 1 \pmod{\text{mgm}(30, 42) = 210}$ att man kan ta $d = 47$.)
Man finner $D(707) \equiv 707^{467} \equiv \cdots \equiv 718$ och $D(615) \equiv 615^{467} \equiv \cdots \equiv 719$

4. Vi gör fermattestet med bas 2: $2^{62} = (2^6)^{10} 2^2 = 64^{10} \cdot 4 \equiv 1^{10} \cdot 4 = 4 \neq 1 \pmod{63}$, så fermattestet ger att 63 inte är ett primtal.

5. Eftersom 101 är ett primtal och $101 \nmid 43$, gäller (Fermats lilla sats) att $43^{100} \equiv 1 \pmod{101}$ och $43^{139802} = (43^{100})^{1398} \cdot 43^2 \equiv 1^{1397} \cdot 1849 \equiv 31 \pmod{101}$.

6. Eftersom $341 = 11 \cdot 31$, där 11 och 31 är primtal, är $\phi(341) = 10 \cdot 30 = 300$. $\text{sgd}(341, 43) = 1$, så (Euler) $43^{300} \equiv 1 \pmod{341}$ och $43^{139802} = (43^{300})^{466} \cdot 43^2 \equiv 1^{466} \cdot 1849 \equiv 144 \pmod{341}$.