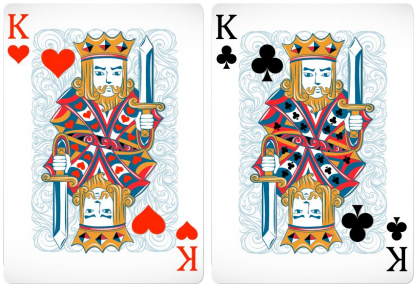
POKER w grudniowy wieczór w Krakowie

Kraków, późna jesień. Żółte światło ulicznych latarni ledwo przebija się przez kłęby szarego dymu. W wodach kałuż leżących na ulicy odbijają się postury studentów powracających na Miasteczko, jednak cztery postacie zmierzają w przeciwnym kierunku. Zgarbione, lekko niepewne, chcące pozostać nierozpoznane wchodzą do małego o dziwnej, a zarazem intrygującej architekturze, żółto-szarego budynku. Są to Vsevolod, Maria, Aneta i Adam. Może nie chcieli dzisiaj tu być, może woleliby być na konferencji we Wiedniu, może chcieliby dzisiaj piec pierniki, ale dzisiaj już muszą, zaryzykować.

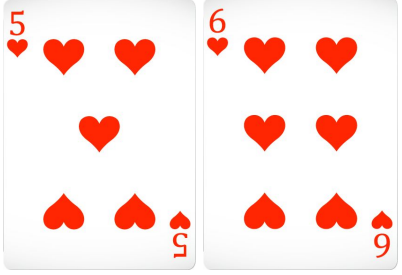
Rozpoczynają grę.
Vsevolod otrzymał dwa króle, kier oraz trefl.



Maria trzyma w ręce waleta karo oraz dziesiątkę karo.

Aneta asa i damę pik.

Adam natomiast piątkę i szóstkę kier.

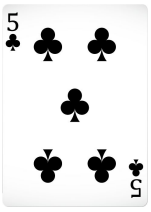


Vsevolod zadowolony ze swoich kart podbił stawkę, ale nawet Adam się nie wycofał. Każdy wie, że dzisiaj nie można sobie pozwolić na przegraną, zbliżają się święta, a prezenty ktoś kupić musi.

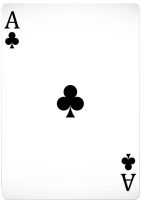
Pierwsze trzy karty pojawiają się na stole:
Co to będzie, co to będzie? Metoda RSA powie Tobie, co za flop to będzie.

1. **karta** [E(l)=120, p=17, q=23, e=7]

375

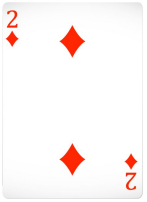


325

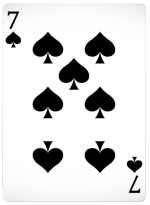


25

2. **karta** [E(l)=74, p=13, q=23, e=245]



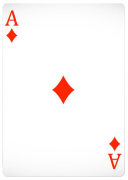
46



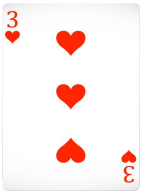
108

42

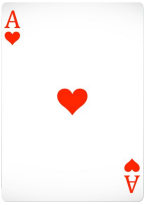
3. **karta** [E(l)=255, p=5, q=61, e=37]



85

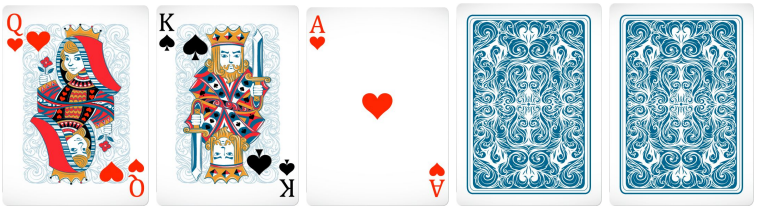


67



255

Zatem pierwsze trzy karty wyglądają następująco:



Vsevolod ma już trójkę i brakuje mu tylko czwartego króla do karety.
Maria ma już pewnego strita, ale bez szans na kolor.
Aneta ma już dwie wysokie pary i może liczyć nawet na królewskiego pokera.
Adam może liczyć tylko na kolor.

Na stole pojawia się **czwarta karta**.
Co to będzie, co to będzie? Spytać Rabina, o odpowiedź musisz.

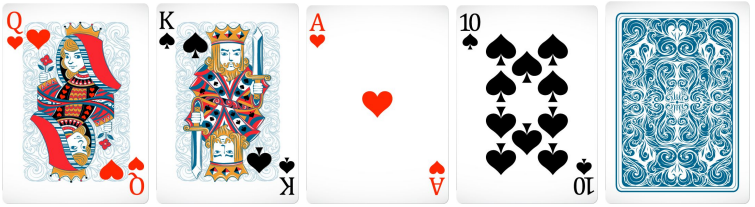
4. **karta** [E(I)=45, p=11, q=19]

145

87

69

Teraz stół wygląda w taki sposób:

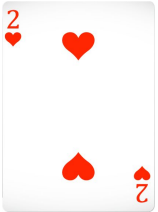


Vsevolodowi wciąż brakuje tylko czwartego króla do karety albo pary na stole do fula.
Maria ma już strita.
Anecie brakuje waleta pik do królewskiego pokera albo pika do koloru albo A lub Q do fulla .
Adamowi wystarczy jeden kier do koloru.

Piąta i ostatnia karta ukazuje się na stole:
Co to będzie, co to będzie? Spytać Rabina, o odpowiedź musisz.

5. **Karta** [E(I)=36, p=43, q=19]

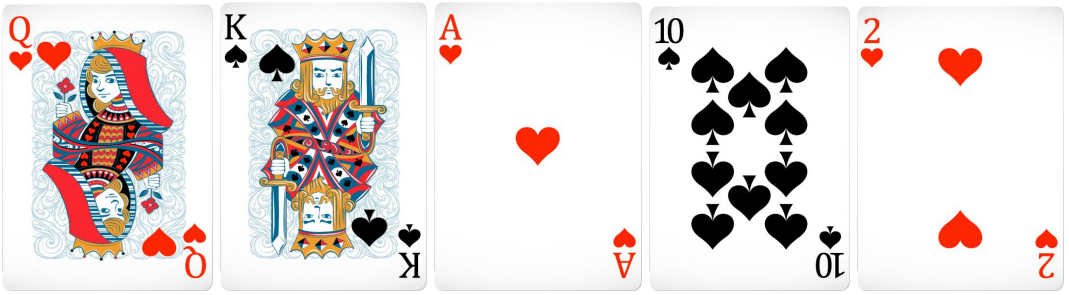
812



424

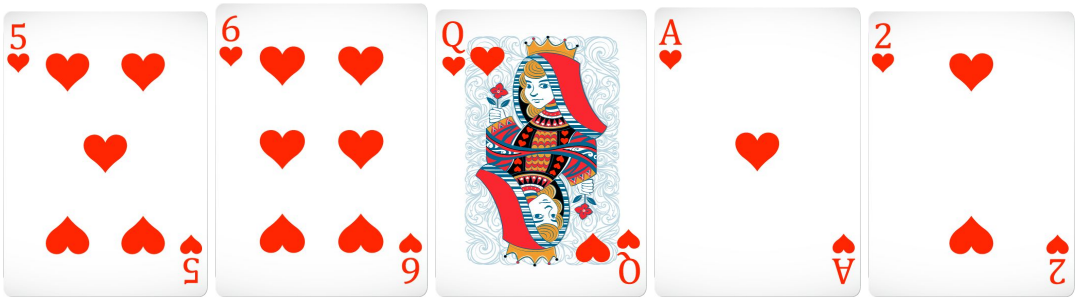
3

Stół ostatecznie wygląda w następujący taki sposób:



Vsevolod ma trójkę króli.
Maria ma strita 10, J, Q, K, A.
Aneta ma dwie pary asów i dam.
Adam ma kolor kier.

Zatem Adam wygrywa i to u niego w domu rodzina nie musi się już martwić o święta.



Ad. karta 1.
Odszyfrujmy liczbę 120:
$p \cdot q = 17 \cdot 23 = 391 = n,\ e = 7$
$\varphi(n) = 16 \cdot 22 = 352$
Znajdźmy $d = 7^{-1}$ w $\mathbb{Z}^*_{352}$ korzystając z algorytmu Euklidesa
$352 = 7 \cdot 50 + 2$
$7 = 2 \cdot 3 + 1$
$1 = 7 - 3 \cdot 2 = 7 - 3 \cdot (352 - 7 \cdot 50) = 151 \cdot 7 - 3 \cdot 352$
$d = 151$
Odszyfrowywanie:
$120^{151}\ (mod\ 391) = (120^{15})^{10}\ (mod\ 391) = 341^{10} \cdot 120\ (mod\ 391) = (-50)^{10} \cdot 120\ (mod\ 391) = 52 \cdot 120\ (mod\ 391) = 375\ (mod\ 391)$

Szyfrowanie:
$l = 375,\ p \cdot q = 17 \cdot 23 = 391 = n$
$\varphi(n) = 16 \cdot 22 = 352$
Wybieramy $e = 7 \perp 352 = \varphi(391)$
Szyfrujemy l:
$E(l) = 375^7\ (mod\ 391) = (-16)^7\ (mod\ 391) = 188 \cdot (-16)\ (mod\ 391) = -271\ (mod\ 391) = 120\ (mod\ 391)$

Ad. karta 2.
Odszyfrujmy liczbę 74:
$p \cdot q = 13 \cdot 23 = 299 = n,\ e = 245$
$\varphi(n) = 12 \cdot 22 = 264$
Znajdźmy $d = 245^{-1}$ w $\mathbb{Z}^*_{264}$ korzystając z algorytmu Euklidesa
$264 = 245 + 19$
$245 = 19 \cdot 12 + 17$
$19 = 17 + 2$
$17 = 8 \cdot 2 + 1$
$1 = 17 - 8 \cdot 2 = 17 - 8 \cdot (19 - 17) = 9 \cdot 17 - 8 \cdot 19 = 9 \cdot (245 - 19 \cdot 12) - 8 \cdot 19 = 9 \cdot 245 - 116 \cdot 19 = 9 \cdot 245 - 116 \cdot (264 - 245) = 125 \cdot 245 - 116 \cdot 264$
$d = 125$
Odszyfrowywanie:
$74^{125}\ (mod\ 299) = ((74^5)^5)^5\ (mod\ 299) = (250^5)^5\ (mod\ 299) = 217^5\ (mod\ 299) = 42\ (mod\ 299)$

Szyfrowanie:
$l = 42,\ p \cdot q = 13 \cdot 23 = 299 = n$
$\varphi(n) = 12 \cdot 22 = 264$
Wybieramy $e = 245 \perp 264 = \varphi(299)$
Szyfrujemy l:
$E(l) = 42^7\ (mod\ 299) = ((42^{10})^{12})^2 \cdot 42^5\ (mod\ 299) = (29^{12})^2 \cdot 126\ (mod\ 299) = 144^2 \cdot 126 (mod\ 299) = 105 * cdot 126\ (mod\ 299) = 74\ (mod\ 299)$

Ad. karta 3.
Odszyfrujmy liczbę 255:
$p \cdot q = 5 \cdot 61 = 305 = n,\ e = 37$
$\varphi(n) = 4 \cdot 60 = 240$
Znajdźmy $d = 37^{-1}$ w $\mathbb{Z}^*_{240}$ korzystając z algorytmu Euklidesa
$240 = 37 \cdot 6 + 18$
$37 = 18 \cdot 2 + 1$
$1 = 37 - 2 \cdot 18 = 37 - 2 \cdot (240 - 37 \cdot 6) = 13 \cdot 37 - 2 \cdot 240$
$d = 13$
Odszyfrowywanie:
$255^{13}\ (mod\ 305) = 255\ (mod\ 305)$

Szyfrowanie:
$l = 255,\ p \cdot q = 5 \cdot 61 = 305 = n$
$\varphi(n) = 4 \cdot 60 = 240$
Wybieramy $e = 37 \perp 240 = \varphi(305)$
Szyfrujemy l: $E(l) = 255^{37}\ (mod\ 305) = ((-50)^{12})^3 \cdot 255\ (mod\ 305) = (245)^3 \cdot 255\ (mod\ 305) = (-60)^3 \cdot (-50)\ (mod\ 305) = (-60) \cdot (-50)\ (mod\ 305) = 255\ (mod\ 305)$

Ad. karta 4.
Odszyfrujmy liczbę 45:
$p \cdot q = 11 \cdot 19 = 209 = n$
$x^2 = 45 \ (mod(11 \cdot 19))$
$\begin{cases} x^2 = 45 \pmod{11} \\ x^2 = 45 \pmod{19} \end{cases}$
$\begin{cases} x^2 = 1 \pmod{11} \\ x^2 = 7 \pmod{19} \end{cases}$
Z pierwszego równania mamy:
$x = 1 \ (mod \ 11) \vee x = 11 - 1 \ (mod \ 11) = 10 \ (mod \ 11)$
Z drugiego równania mamy:
$x = 7^{\frac{19+1}{4}} \ (mod \ 19) \vee x = 19 - 7^{\frac{19+1}{4}} \ (mod \ 19)$
$x = 11 \ (mod \ 19) \vee x = 8 \ (mod \ 19)$
Ostatecznie $x \in \{1, 10\}$ w $\mathbb{Z}_{11}, \ x \in \{11, 8\}$ w $\mathbb{Z}_{19}$
$x_1 : \begin{cases} x = 1 \pmod{11} \\ x = 11 \pmod{19} \end{cases} \qquad x_2 : \begin{cases} x = 1 \pmod{11} \\ x = 8 \pmod{19} \end{cases}$
$x_3 : \begin{cases} x = 10 \pmod{11} \\ x = 11 \pmod{19} \end{cases} \qquad x_4 : \begin{cases} x = 10 \pmod{11} \\ x = 8 \pmod{19} \end{cases}$
Znajdźmy x_1 :
$\begin{cases} x = 1 \pmod{11} \\ x = 11 \pmod{19} \end{cases}$
Wyliczmy x z drugiego równania i wstawmy do pierwszego
$x = 11 + 19k, \ k \in \mathbb{N}$
$11 + 19k = 1 \ (mod \ 11)$
$8k = 1 \ (mod 11) \ / \cdot 7 \ (8^{-1} = 7 \text{ w } \mathbb{Z}_{11}^*)$
$k = 7 \ (mod \ 11) \implies k = 7 + 11l, \ l \in \mathbb{N}$
Wracamy do równania $x = 11 + 19k$ i otrzymujemy
$x = 11 + 19(7 + 11l) \ (mod \ 209)$
$x = 144 \ (mod \ 209) \qquad x_1 = 144$
Znajdźmy x_4 :
$x_4 = 209 - 144 = 65$
Znajdźmy x_3 :
$\begin{cases} x = 10 \pmod{11} \\ x = 11 \pmod{19} \end{cases}$
Wyliczmy x z drugiego równania i wstawmy do pierwszego
$x = 8 + 19k, \ k \in \mathbb{N}$
$8 + 19k = 1 \ (mod \ 11)$
$8k = 4 \ (mod 11) \ / \cdot 7 \ (8^{-1} = 7 \text{ w } \mathbb{Z}_{11}^*$
$k = 6 \ (mod \ 11) \implies k = 6 + 11l, \ l \in \mathbb{N}$
Wracamy do równania $x = 8 + 19k$ i otrzymujemy
$x = 8 + 19(6 + 11l) \ (mod \ 209)$
$x = 122 \ (mod \ 209) \qquad x_3 = 122$
Znajdźmy x_2 :
$x_2 = 209 - 122 = 87$
Ostatecznie $x \in \{144, \ 87, \ 122, \ 65\}$

Szyfrowanie:
$l = 87, \ p \cdot q = 11 \cdot 19 = 209 = n$
Szyfrujemy l: $E(l) = 87^2 \ (mod \ 209) = 45 \ (mod \ 209)$

Ad. karta 5.
Odszyfrujmy liczbę 36:
$p \cdot q = 43 \cdot 19 = 817 = n$
$x^2 = 36 \ (mod(43 \cdot 19))$
$\begin{cases} x^2 = 36 \pmod{43} \\ x^2 = 36 \pmod{19} \end{cases}$
$\begin{cases} x^2 = 36 \pmod{43} \\ x^2 = 17 \pmod{19} \end{cases}$
Z pierwszego równania mamy:
$x = 36^{\frac{43+1}{4}} \ (mod \ 43) \vee x = 43 - 36^{\frac{43+1}{4}} \ (mod \ 43)$
$x = (-7)^{11} \ (mod \ 43) \vee x = 43 - (-7)^{11} \ (mod \ 43)$
$x = 37 \vee x = 6$
Z drugiego równania mamy:
$x = 7^{\frac{19+1}{4}} \ (mod \ 19) \vee x = 19 - 7^{\frac{19+1}{4}} \ (mod \ 19)$
$x = 11 \ (mod \ 19) \vee x = 8 \ (mod \ 19)$
Ostatecznie $x \in \{6, 37\}$ w $\mathbb{Z}_{43}, \ x \in \{6, 13\}$ w $\mathbb{Z}_{19}$
$x_1 : \begin{cases} x = 6 \pmod{43} \\ x = 6 \pmod{19} \end{cases} \qquad x_2 : \begin{cases} x = 6 \pmod{43} \\ x = 13 \pmod{19} \end{cases}$
$x_3 : \begin{cases} x = 37 \pmod{43} \\ x = 7 \pmod{19} \end{cases} \qquad x_4 : \begin{cases} x = 37 \pmod{43} \\ x = 13 \pmod{19} \end{cases}$
Znajdźmy x_1 :
$\begin{cases} x = 6 \pmod{43} \\ x = 6 \pmod{19} \end{cases}$
Wyliczmy x z drugiego równania i wstawmy do pierwszego
$x = 6 + 19k, \ k \in \mathbb{N}$
$6 + 19k = 6 \ (mod \ 43)$
$19k = 0 \ (mod 43)$
$k = 0 \ (mod \ 43) \implies k = 43l, \ l \in \mathbb{N}$
Wracamy do równania $x = 6 + 19k$ i otrzymujemy
$x = 6 + 19 \cdot 43l \ (mod \ 817)$
$x = 6 \ (mod \ 817) \qquad x_1 = 6$
Znajdźmy x_4 :
$x_4 = 817 - 6 = 811$
Znajdźmy x_2 :
$\begin{cases} x = 6 \pmod{43} \\ x = 13 \pmod{19} \end{cases}$
Wyliczmy x z drugiego równania i wstawmy do pierwszego
$x = 13 + 19k, \ k \in \mathbb{N}$
$13 + 19k = 6 \ (mod \ 43)$
$19k = -7 \ (mod 43) \ / \cdot (-9) \ (19^{-1} = -9 \text{ w } \mathbb{Z}_{43}^*$
$k = 20 \ (mod \ 43) \implies k = 20 + 43l, \ l \in \mathbb{N}$
Wracamy do równania $x = 13 + 19k$ i otrzymujemy
$x = 13 + 19(20 + 43l) \ (mod \ 817)$
$x = 393 \ (mod \ 817) \qquad x_2 = 393$
Znajdźmy x_3 :
$x_3 = 817 - 393 = 424$
Ostatecznie $x \in \{6, \ 393, \ 424, \ 811\}$

Szyfrowanie:
$l = 424, \ p \cdot q = 43 \cdot 19 = 817 = n$
Szyfrujemy l: $E(l) = 424^2 \ (mod \ 817) = 36 \ (mod \ 817)$