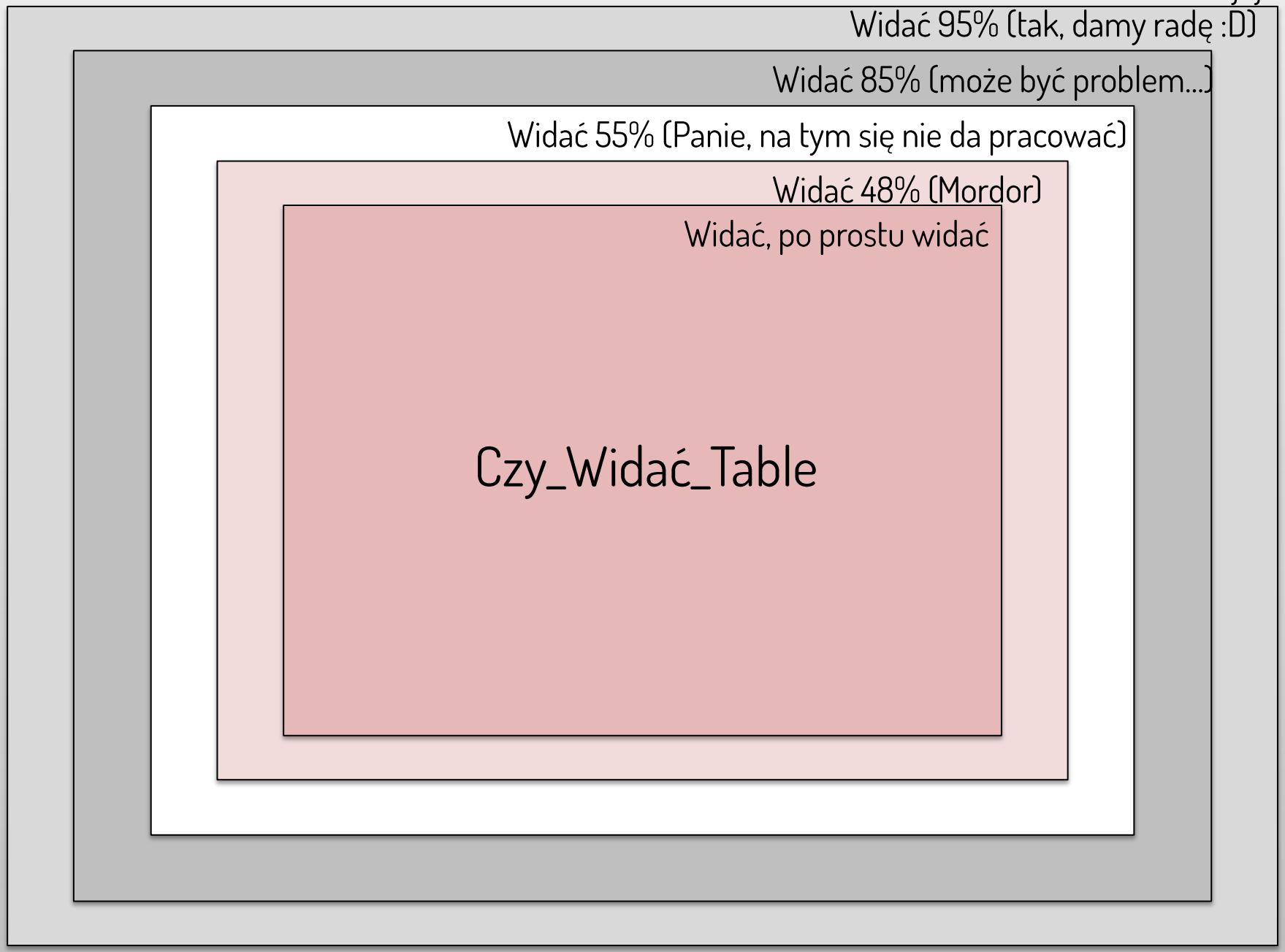

Widać 100% (jej :D)
Widać 95% (tak, damy radę :D)
Widać 85% (może być problem...)
Widać 55% (Panie, na tym się nie da pracować)
Widać 48% (Mordor)
Widać, po prostu widać
Czy_Widać_Table

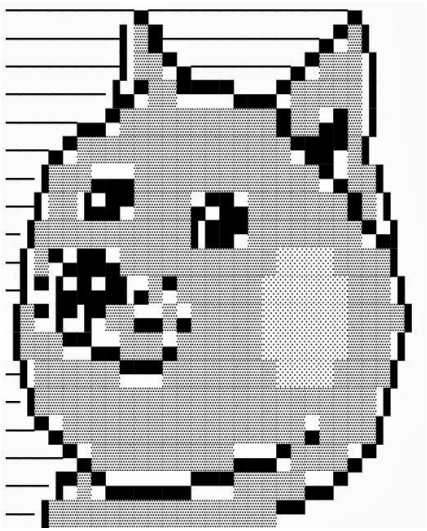
RSA

Prezentacja (chyba)

RSA -> |
\/

← //To są strzałki

Algorytm Rivesta–Shamira–Adlemana



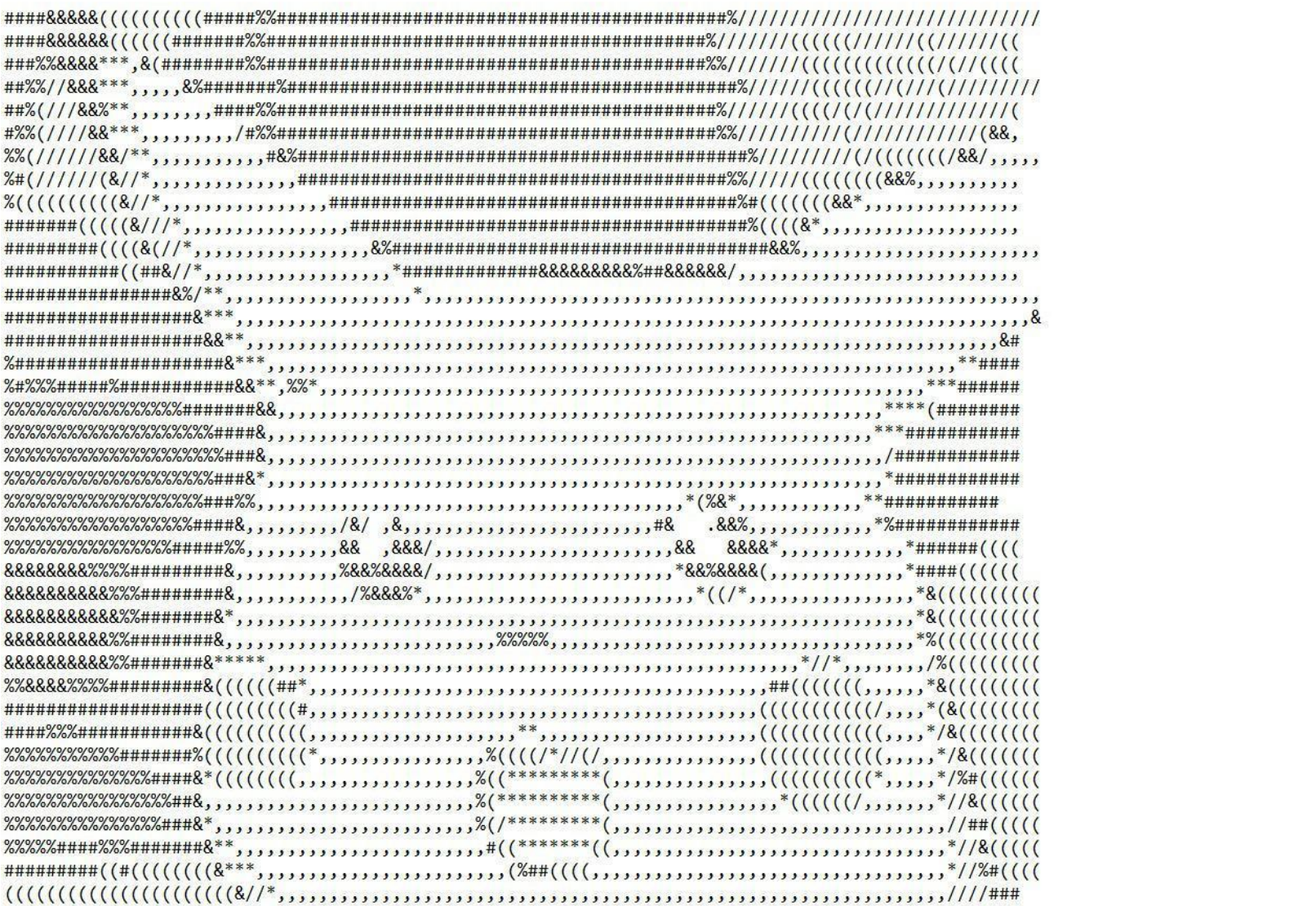
¿ RSA jakie jest, każdy widzi.?

- Jest to jeden z pierwszych i obecnie najpopularniejszych asymetrycznych algorytmów kryptograficznych z kluczem publicznym, zaprojektowany w 1977 przez Rona Rivesta, Adiego Shamira oraz Leonarda Adlemana

Reddit : You can't make memes in Notepad

Me : *makes meme in notepad*

Reddit :



Opis algorytmu, (czyli czym to się je)

edit: (proszę nie mówić, że łyżeczką)

edit2: (tak naprawdę widelcem)

E-dit3: (Tak serio serio to łyżdelec)

Opis algorytmu

1) Wybieramy losowo dwie DUŻE liczby pierwsze p , q
np. p = 2, q = 3

Dwa) Obliczamy N = p * q;

Ƹ) Obliczamy wartość funkcji Eulera: $\varphi(N) = (p - 1)(q - 1)$

„O cholera to funkcja Eulera"
~ Wiadomo kto

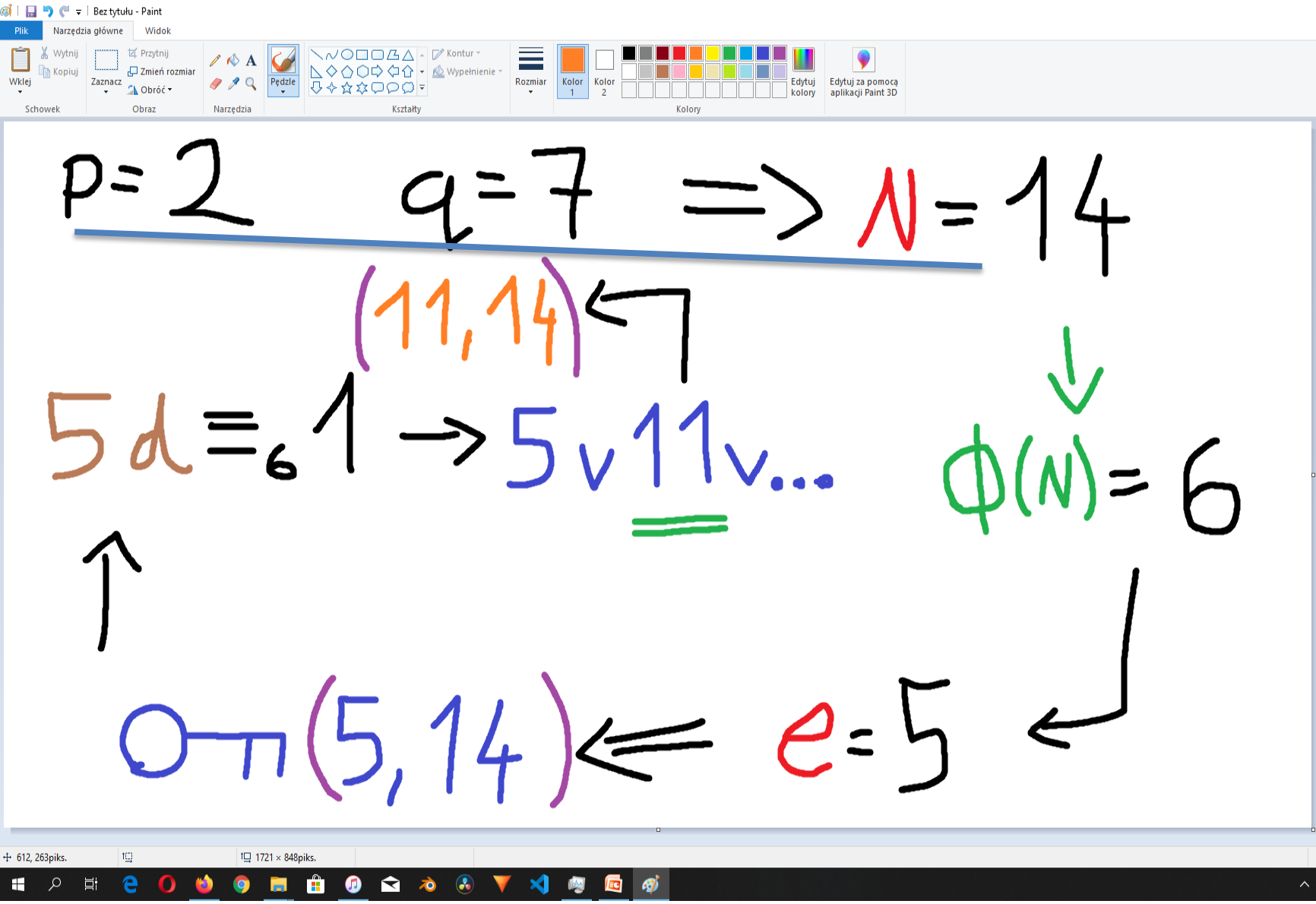
4. Wybieramy liczbę e: $\begin{cases} 1 < e < \varphi(N) \\ NWD(e, \varphi(N)) = 1 \end{cases}$

5} Klucz publiczny = (e, N)

6. Wybieramy liczbę d taką, że $(d*e) \bmod(\varphi(N)) = 1$

ƧЄVЄᑎ Klucz prywatny -> (d , N)

Example:


Bez tytułu - Paint
Plik
Narzędzia główne
Widok
Wklej
Wytnij
Kopiuj
Zaznacz
Przytnij
Zmień rozmiar
Obróć
Pędzle
Kontur
Wypełnienie
Rozmiar
Kolor 1
Kolor 2
Edytuj kolory
Edytuj za pomocą aplikacji Paint 3D
Schowek
Obraz
Narzędzia
Kształty
Kolory
p=2 q=7 ⇒ N=14
(11,14)
5d ≡6 1 → 5v11v...
φ(N)=6
e=5
(5,14)
612, 263piks.
1721 × 848piks.
100%
22:44
17.11.2019

SZYFROWANIE

(Na przykładzie p = 2, q = 7)

Klucz publiczny: (5 , 14)
Wiadomość: „B”

$$B \rightarrow 2 \rightarrow 2^5 mod(14) = 32 mod(14) = 4 \rightarrow D$$

DESZYFROWANIE

(Na przykładzie p = 2, q = 7)

Klucz prywatny: (11 , 14)
Wiadomość: „D”

$$D \to 4 \to \quad 4^{11} mod(14) = \ 4194304 mod(14) = \ 2 \to B$$

Własności

Niech $C_{K_1}, D_{K_1}, C_{K_2}, D_{K_2}$ będą kolejno szyfrowaniem i deszyfrowaniem kluczami K_1 i K_2. Wtedy zachodzi:

- $C_{K_1}\left(C_{K_2}(M)\right) = C_{K_2}\left(C_{K_1}(M)\right)$ - przemienność operacji szyfrowania
- $D_{K_1}\left(D_{K_2}(M)\right) = D_{K_2}\left(D_{K_1}(M)\right)$ - przemienność operacji deszyfrowania

!! Ze względów bezpieczeństwa nie powinno się stosować więcej niż 2 zagnieżdżone szyfrowania ze względu na ataki oparte na chińskim twierdzeniu o resztach.

Ciekawostki

Dotychczas największym kluczem RSA, jaki rozłożono na czynniki pierwsze, jest klucz 768-bitowy

Dziękuję za uwagę!