

Pytanie 1

Dla algorytmu RSA z kluczem prywatnym $p=3$, $q=5$ oraz publicznym $e=3$ deszyfrować kryptogram $C=2$.

Odpowiedź: 8

Pytanie 2

Za pomocą schematu Schnorra wygenerować podpis tekstu $x=1$, używając funkcję haszującą $H(x)=x$, gdzie $(p=7, q=3, h=2, n=4)$ – klucz publiczny $(a=4, r=2)$ – klucz prywatny. Pobrać liczbę weryfikującą ten podpis.

Odpowiedź: 14

Pytanie 3

Za pomocą schematu Schnorra wygenerować podpis tekstu $x=3$, używając funkcję haszującą $H(x)=x$, gdzie $(p=7, q=3, h=2, n=4)$ – klucz publiczny $(a=4, r=2)$ – klucz prywatny. Pobrać liczbę weryfikującą ten podpis.

Odpowiedź: 34

Pytanie 4

Przy użyciu szyfru stumieniowego na podstawie generatora RSA liczb pseudolosowych dla $n=21$, $e=5$ oraz zarodku $x_0=3$ deszyfrować kryptogram $(0, 0, 0)$.

Odpowiedź: $(0, 1, 0)$

Pytanie 5

Za pomocą schematu ElGamala z kluczem publicznym $p=7$, $g=2$, $h=2$ oraz prywatnym $a=4$ deszyfrować kryptogram $C=(2,3)$.

Odpowiedź: ~~5~~ 4

Pytanie 6

Czy liczba 5 jest generatorem zbioru Z_{13} ?

Odpowiedź: Fałsz

Pytanie 7

Czy za pomocą szyfru par z kluczem „Kaszanka dla wszystkich” można szyfrować teksty w języku angielskim?

Odpowiedź: Prawda

Pytanie 8

Ilość warstw algorytmu AES

Odpowiedź: 4

Pytanie 9

Czy algorytm One-time pad przewiduje wykorzystanie autoklucza?

Odpowiedź: Fałsz

Pytanie 10

Obliczyć $3^{-1} \bmod 14$

Odpowiedź: 5

Pytanie 11

Obliczyć $\phi(2^{127}-1)$, $\phi(33)$, gdzie ϕ jest funkcją Eulera.

Odpowiedź: $(2^{127}-2, 20)$

Pytanie 12

Długość klucza algorytmu DESX

Odpowiedź: 192

Pytanie 13

Za pomocą szyfru Hilla dla ilości liter alfabetu $n=26$ deszyfrować kryptogram (7, 17), gdzie

$K = \begin{pmatrix} 1 & 16 \\ 1 & 21 \end{pmatrix}$

jest kluczem szyfru.

Odpowiedź: (1, 2)

Pytanie 14

Obliczyć $(x^8 + x^5)^2$ w zbiorze $F_2[x]$

Odpowiedź: $(x^5 + x^4 + x)$

Pytanie 15

Maksymalna długość bloku szyfrowania algorytmem AES

Odpowiedź: 256

Pytanie 16

Znaleźć wszystkie pierwiastki $\sqrt[3]{1} \bmod n$, $n=7 \times 9$

Odpowiedź: (1, 8, 55, 62)

Pytanie 17

Za pomocą szyfru strumieniowego na podstawie generatora RSA liczb pseudolosowych dla $n=35$, $e=5$ oraz zarodku $x_0=3$ zaszyfrować ciąg bitów (1, 1, 0).

Odpowiedź: (0, 0, 1)

Pytanie 18

Czy liczba 5 należąca do \mathbb{Z}^*_{11} jest resztą kwadratową?

Odpowiedź: Prawda

Pytanie 19

Długość klucza algorytmu DES EDE

Odpowiedź: 108

Pytanie 20

Obliczyć $3^{-1} \bmod 14$

Odpowiedź: 5

Pytanie 21

Czy liczba 5 jest generatorem zbioru \mathbb{Z}_{13}^* ?

Odpowiedź: Fałsz

Pytanie 22

Za pomocą algorytmu p-1 Pollarda sfaktoryzować liczbę $n=35$. Podać niezbędną ilość kroków algorytmu faktoryzacji.

Odpowiedź: 2

Pytanie 23

Dla schematu DSA wygenerować podpis tekstu 1221 używając funkcję kaszującą $H(x)=1$, gdzie $(p=7, q=3, h=2)$ – klucz publiczny $(a=2, r=1)$ – klucz prywatny. Podać parę liczb tworzących ten podpis.

Odpowiedź: (2,2)

Pytanie 24

Za pomocą szyfru strumieniowego na podstawie generatora Blum-Micali dla $a=2, p=7$ oraz zarodku $x_0=5$ zaszyfrować ciąg bitów (0, 1, 0).

Odpowiedź: (1, 1, 1)

Pytanie 25

Za pomocą schematu Schnorra wygenerować podpis cyfrowy tekstu $x=2$, używając funkcję haszującą $H(x)=x$, gdzie $(p=7, q=3, h=2, n=4)$ – klucz publiczny $(a=4, r=2)$ – klucz prywatny. Podać liczbę weryfikującą ten podpis.

Odpowiedź: 24

Pytanie 27

Minimalna długość bloku szyfrowania algorytmem AES

Odpowiedź: 128

Pytanie 28

Dla kryptosystemu M. Rabina z kluczem prywatnym $p=3, q=11$ deszyfrować kryptogram $C=31$.

Odpowiedź: (8,14,19,25)

Pytanie 29

Obliczyć $3^{-1} \bmod 15$

Odpowiedź: brak

Pytanie 30

Znaleźć, jeżeli są, wszystkie pierwiastki $\sqrt{1} \bmod n$, $n=7 \times 11$

Odpowiedź: (1, 34, 43, 76)

Pytanie 31

Za pomocą algorytmu „Sito kwadratowe” sfaktoryzować liczbę $n=21$, używając funkcji $f(X)=(X+\sqrt{n})^2-n$. Podać wartości X , które definiują decydującą kongruencję.

Odpowiedź: (-3, 0)

Pytanie 32

Znaleźć liczbę naturalną x taką, że $x \equiv 1 \pmod{12}$, $x \equiv 5 \pmod{7}$.

Odpowiedź: 145

Pytanie 33

Znaleźć wszystkie pierwiastki $\sqrt{5} \bmod n$, $n=3 \times 11$

Odpowiedź: brak

Pytanie 34

Za pomocą algorytmu $p-1$ Pollarda sfaktoryzować liczbę $n=55$. Podać niezbędną ilość kroków algorytmu faktoryzacji.

Odpowiedź: 3

Pytanie 35

Czy może reszta kwadratowa zbioru \mathbb{Z}^*_p być generatorem tego zbioru?

Odpowiedź: Fałsz

Pytanie 36

Czy procedura $\text{xtime}(a)$ jest używana przy obliczeniach MixColumn algorytmu AES?

Odpowiedź: ~~Fałsz~~ Prawa

Pytanie 37

Za pomocą schematu ElGamala z kluczem publicznym $p=7$, $g=2$, $h=2$ oraz prywatnym $a=4$ deszyfrować kryptogram $C=(2,1)$.

Odpowiedź: 4

Pytanie 38

$$\overline{DES_K(M)} = DES_{\overline{K}}(\overline{M})$$

Czy zachodzi równość dla algorytmu DES, gdzie M – tekst jawny, K -klucz, a kreska oznacza negację bitów?

Odpowiedź: Prawda

Pytanie 39

Za pomocą algorytmu Blum-Goldwasser na podstawie generatora BBS dla $p=7$, $q=11$ oraz zarodku $x_0=3$ deszyfrować kryptogram $(0, 1, 0; 25)$.

Odpowiedź: (1, 1, 1)

Pytanie 40

Dla kryptosystemu M. Rabina z kluczem prywatnym $p=3$, $q=19$ deszyfrować kryptogram $C=7$.

Odpowiedź: (8,11,46,49)

Pytanie 41

Znaleźć liczbę naturalną x taką, że $x \equiv 3 \pmod{13}$, $x \equiv 2 \pmod{12}$.

Odpowiedź: 146