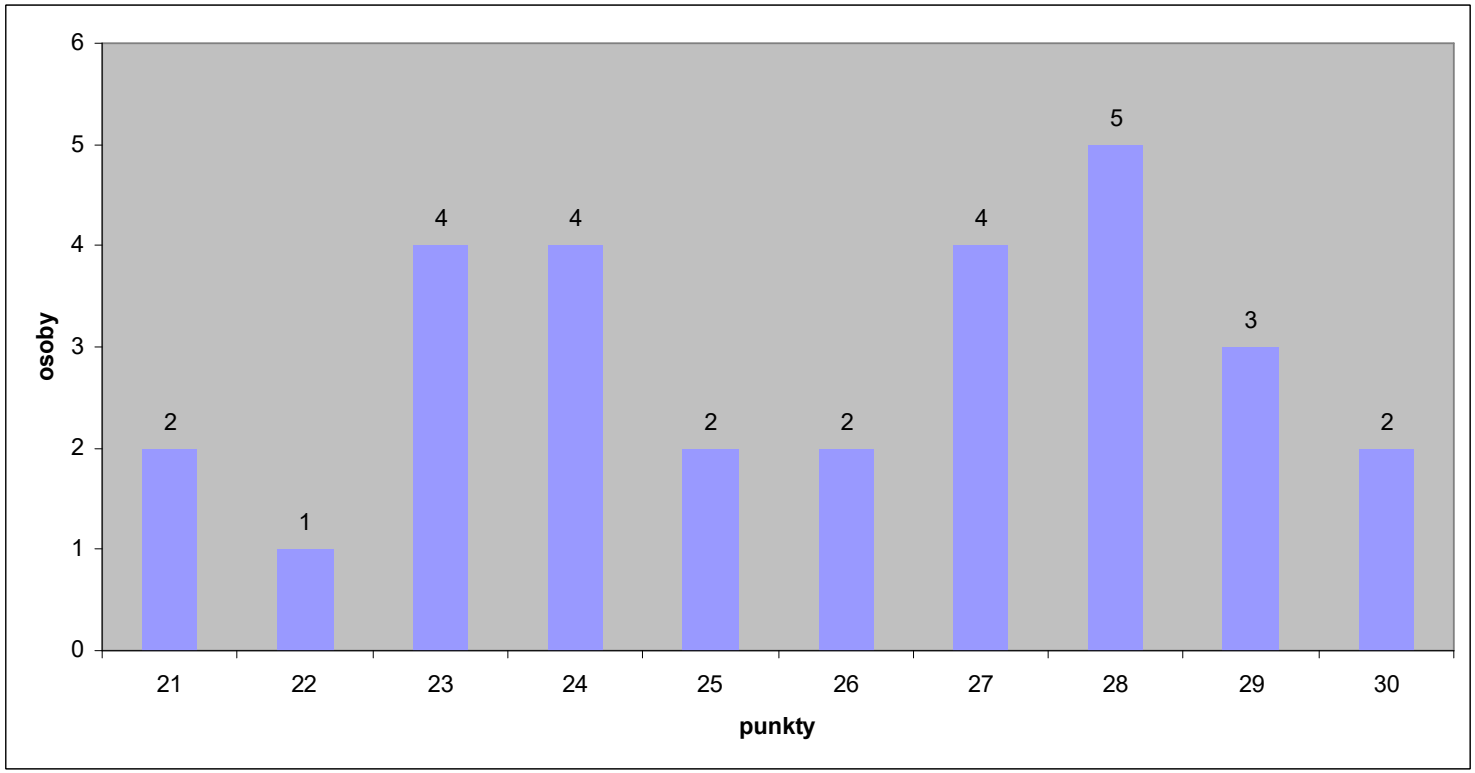
Zaliczenie

Wyniki testu – max 32 punkty



Oceny

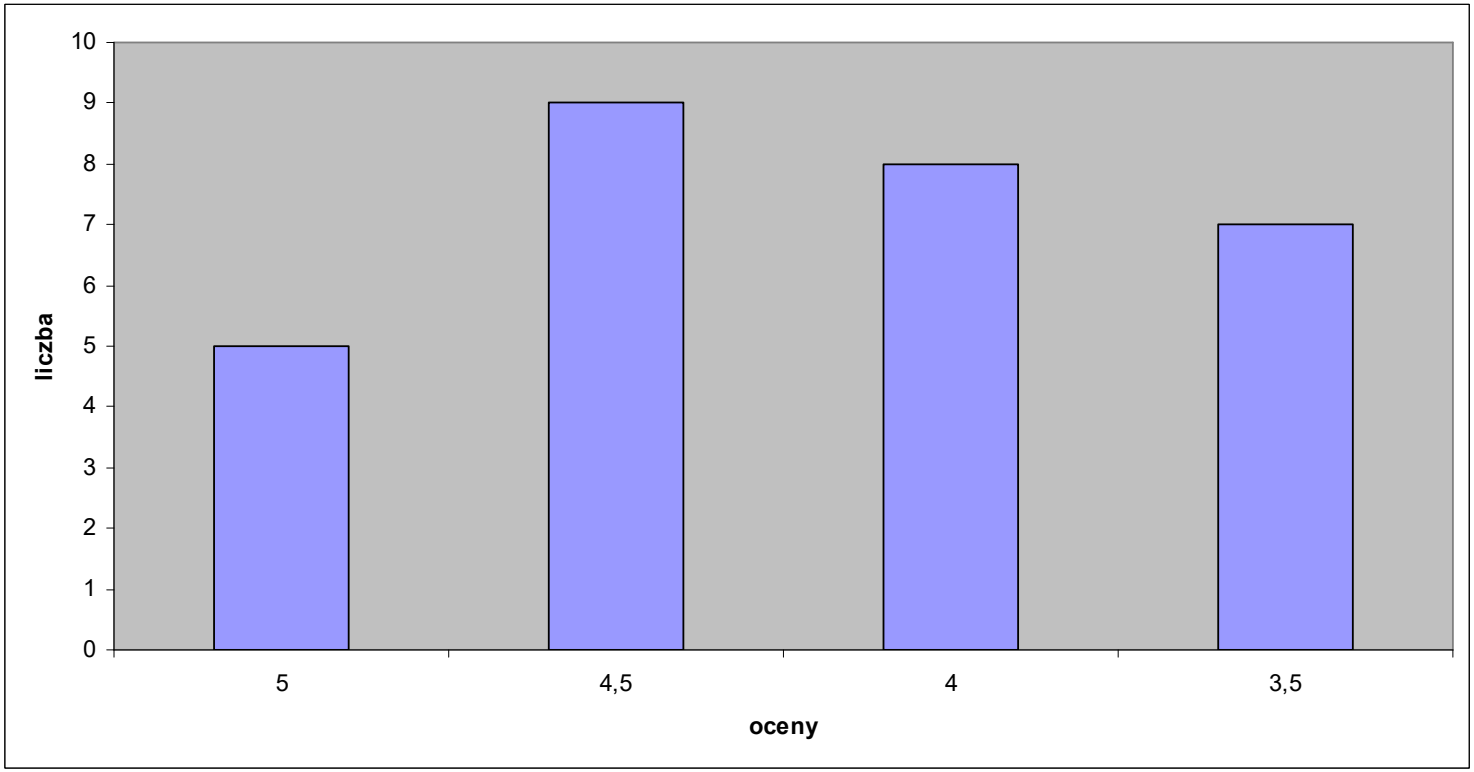
21-23 –> 3,5

24-26 -> 4

27-28 -> 4,5

29-30 -> 5

Oceny proponowane



Poprawa (odp. dobre:23/złe:6)

Który proces weryfikuje tożsamość użytkownika?

a) Identyfikacja

b) Uwierzytelnianie

c) Autoryzacja

Poprawa (28/1)

Które państwo używało do szyfrowania maszynę szyfrującą Enigma?

a) Niemcy

b) Polska

c) Wielka Brytania

d) Stany Zjednoczone

Poprawa (26/2)

Co to jest szyfr symetryczny?

a) Szyfr, w którym używany jest jeden klucz do zarówno szyfrowania, jak i deszyfrowania danych

b) Szyfr, który wykorzystuje dwa różne klucze: publiczny i prywatny

c) Szyfr, który korzysta z algorytmów opartych na funkcjach skrótu

d) Szyfr, który wykorzystuje sekwencję losowych liczb do kodowania danych

Poprawa (7/22)

Który z poniższych standardów jest obecnie najczęściej stosowany jako algorytm szyfrowania symetrycznego?

a) RSA

b) Idea

c) AES

d) ECC

Poprawa (18/11)

Jakie jest zastosowanie kryptografii asymetrycznej i symetrycznej w procesie szyfrowania?

a) Kryptografia asymetryczna szyfruje wiadomość, a kryptografia symetryczna szyfruje klucz

b) Kryptografia asymetryczna szyfruje klucz, a kryptografia symetryczna szyfruje wiadomość

c) Kryptografia asymetryczna i symetryczna szyfrują wiadomość jednocześnie

Poprawa (21/8)

Co to jest funkcja skrótu?

a) Matematyczny algorytm, który przekształca dane wejściowe o zmiennej długości na stały wynik o stałej długości

b) Algorytm do szyfrowania danych z wykorzystaniem dwóch kluczy: publicznego i prywatnego

c) Metoda kompresji danych w celu zwiększenia przepustowości sieci

d) Protokół komunikacji sieciowej zapewniający poufność i integralność danych

Poprawa (23/6)

Jakie są główne cechy zapewniane przez podpis cyfrowy?

a) Integralność, autoryzacja pochodzenia, szyfrowanie

b) Integralność, autentyczność pochodzenia, niezaprzeczalność

c) Poufność, autentyczność pochodzenia, integralność

d) Autoryzacja, niezaprzeczalność, szyfrowanie

Poprawa (25/4)

Co zrobi ta komenda? "echo -n „Cześć W pierwszych słowach…" | openssl dgst -sha256 -mac hmac -macopt hexkey:01020304

a) Wygeneruje skrót (hasz) dla tekstu "Cześć W pierwszych słowach...".

b) Wygeneruje skrót (hasz) dla tekstu "Cześć W pierwszych słowach..." z kluczem szesnastkowym 01020304.

c) Obliczy kontrolną sumę dla tekstu "Cześć W pierwszych słowach..." za pomocą funkcji skrótu SHA-256 i algorytmu HMAC, używając klucza w postaci szesnastkowej: 01020304.

d) Zaszyfruje tekst "Cześć W pierwszych słowach..." przy użyciu algorytmu SHA-256 i HMAC z kluczem w postaci szesnastkowej 01020304.

Poprawa (16/13)

(Uwaga pytanie wielokrotnego wyboru) Co to jest certyfikat klucza publicznego?

a) Dokument potwierdzający autentyczność klucza prywatnego

b) Dokument potwierdzający autentyczność klucza publicznego

c) Dokument zawierający klucz prywatny

d) Dokument zawierający klucz publiczny

Poprawa (22/7)

Czym jest "zero day" exploit?

a) Aplikacją komputerową o nowatorskiej funkcjonalności

b) Exploitem wykorzystującym luki w zabezpieczeniach, które są znane od długiego czasu

c) Exploitem wykorzystującym luki w zabezpieczeniach, które są znane od dnia ich odkrycia

d) Zabezpieczeniem przed atakami wykorzystującymi luki zero day

Poprawa (8/21)

W jaki sposób technologia blockchain zapewnia bezpieczeństwo transakcji?

a) Wykorzystuje funkcje skrótu do szyfrowania danych transakcji

b) Umożliwia anonimowość uczestników transakcji

c) Zastosowanie kryptografii asymetrycznej do podpisu cyfrowego transakcji

d) Wykorzystuje analizę ryzyka do oceny bezpieczeństwa transakcji