



„EUROELEKTRA”
Ogólnopolska Olimpiada Wiedzy Elektrycznej i Elektronicznej
Rok szkolny 2018/2019

Zadania z teleinformatyki na zawody III stopnia
z rozwiązaniami

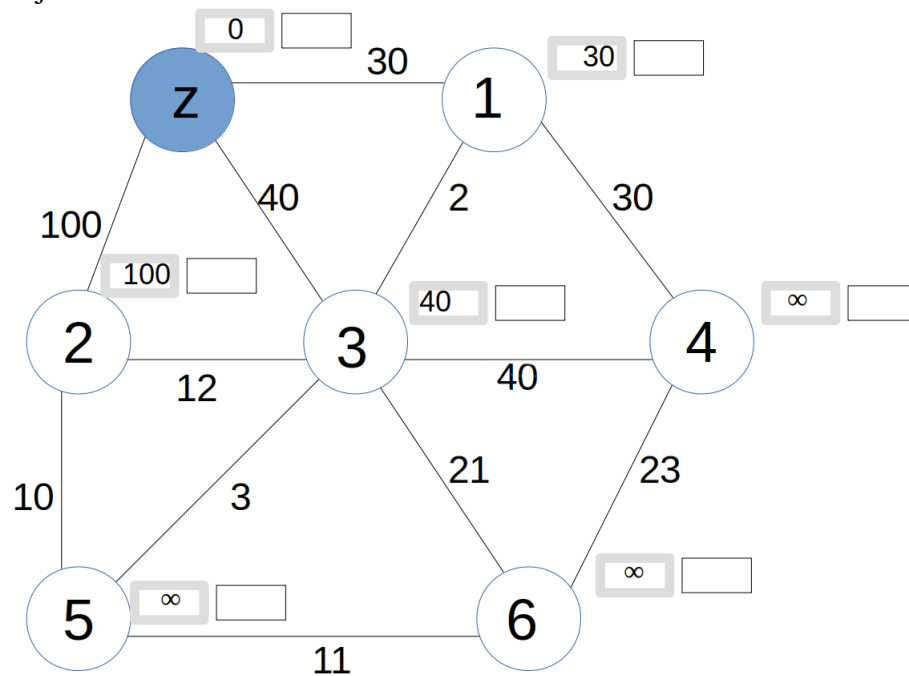
Instrukcja dla zdającego

1. Czas trwania zawodów: 120 minut.
2. III stopień Olimpiady zawiera 6 zadań otwartych.
3. Należy podać poprawną odpowiedź wraz tokiem rozwiązania.
4. Za każdą prawidłową odpowiedź uzyskuje się maksymalnie 10 punktów. Maksymalna liczba punktów do zdobycia za 6 zadań to 60 punktów.
5. Można korzystać z przyborów do pisania, rozdawanych kart czystopisu i brudnopisu, kalkulatorów i tablic matematycznych. Korzystanie z notebooków, tabletów, telefonów komórkowych, smartfonów, smartwatchy, kalkulatorów programowalnych, itp. jest zabronione.

Życzymy powodzenia!

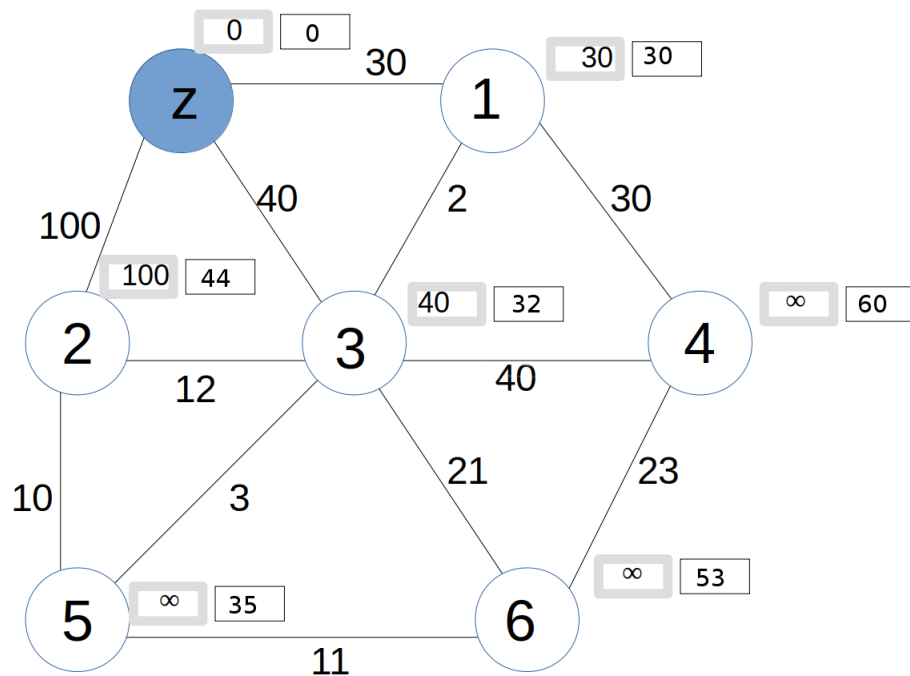
Lp.	Zadanie
1.	<p>Poniżej zaprezentowano algorytm Dijkstry, który wykrywa wszystkie najkrótsze ścieżki w grafie pomiędzy wybranym wierzchołkiem a wszystkimi pozostałymi oraz koszt przejścia każdej z tych ścieżek.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"><pre>AlgorytmDijkstra(G,w,s): Parametry wejściowe: G -graf; z -wierzchołek źródłowy, e(i,j) -koszt krawędzi i,j - w grafie. Utwórz tablicę D odległości od źródła dla wszystkich wierzchołków grafu; Utwórz tablicę P przedników; Dla każdego wierzchołka v w grafie G wykonaj d[v] := nieskończoność p[v] := niezdefiniowane d[s] := 0 na razie są niekolorowane wierzchołki: u:=wierzchołek v o minimalnej wartości d[v] Dla każdego wierzchołka v - sąsiada u: Jeżeli d[v] > d[u] + e(u, v) to: d[v] := d[u] + w(u, v) p[v] := u Koloruj wierzchołek u; Koniec;</pre></div>

Na rys.1 w komórkach szarego koloru, są prezentowane wyniki (koszty wykrytych najkrótszych tras) po pierwszej iteracji. Wpisz w czarne komórki (puste) koszty tras po trzeciej iteracji.



Rys. 1. Graf do zadania 1

Odpowiedź



Rys. 1. Graf do zadania 1

2. Kodowanie Base-64 to popularny sposób przekształcenia informacji tak, aby zawierała wyłącznie podstawowe, drukowalne znaki systemu ASCII. Dzięki tej operacji można bezpiecznie przetwarzać wszelkie znaki specjalne (np. polskie znaki diakrytyczne – ą, ć, ę) oraz znaki posiadające w wielu systemach znaczenie specjalne (&, :, ! itp.). Kodowanie nosi nazwę Base-64, ponieważ zbiór możliwych znaków liczy 64 (2^6) elementy, w odróżnieniu od typowego kodowania ASCII o zbiorze 256 (2^8) możliwości na każdy pojedynczy znak. Różnica w wielkościach zbiorów skutkuje wydłużeniem ciągu ASCII zakodowanego w formacie Base-64.
Przykład: ciągowi „Hej” odpowiada zapis Base-64: „SGVq”, czyli 3x8 bitów zajmuje 4

symbole Base-64 po 6 bitów każdy.
Korzystając z tablicy znaków Base-64 (tabela 1) zdekoduj podany ciąg.

Tabela. 2. Tablica znaków kodowania Base-64

Indeks	Znak	Indeks	Znak	Indeks	Znak	Indeks	Znak
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Ciąg do zdekodowania:

UG93b2R6ZW5pYSB3c3p5c3RraW0gb2xpbXBpamN6eWtvbSE=

Odpowiedź

$U = 20_{10} = 010100_2$

$G = 6_{10} = 000110_2$

$9 = 61_{10} = 111101_2$

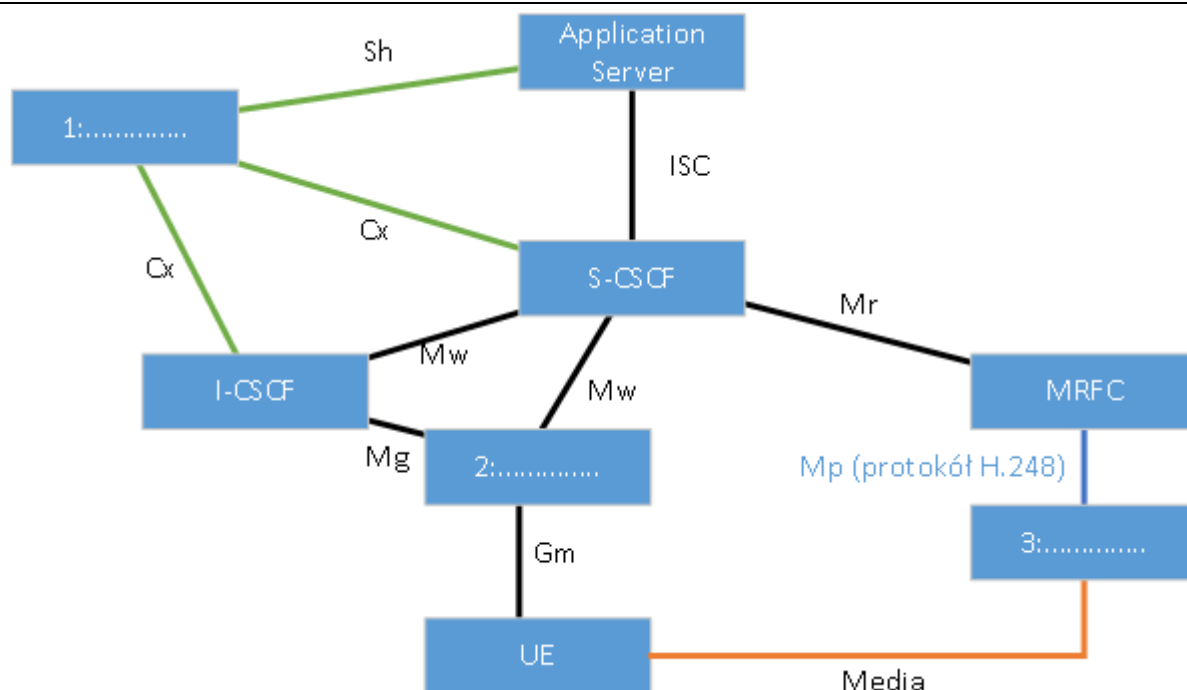
$3 = 55_{10} = 110111_2$

Zatem ciąg 01010000 01101111 01110111 to „Pow”, dekodując analogicznie kolejne znaki otrzymuje się zdanie:

Powodzenia wszystkim olimpijczykom!

3. W pierwszych wersjach standardu IEEE 802.11 stanowiącego podstawę popularnych dziś rozwiązań bezprzewodowych sieci lokalnych WiFi, wykorzystywano zbiór mechanizmów zabezpieczeń określany jako Wired Equivalent Privacy (WEP). Jest on obecnie uznawany obecnie za nie spełniający oczekiwań i został zastąpiony mechanizmami Wireless Protected Access w wersji 2 lub 3 (WPA2 lub WPA3). Opisz najważniejsze różnice pomiędzy rozwiązaniami WEP i WPA2, w szczególności odnoszące się do rodzaju zastosowanego algorytmu szyfrującego, sposobów zapewnienia poufności i integralności przesyłanych danych oraz sposobu generowania kluczy wykorzystywanych przez algorytm szyfrujący.

	Odpowiedź	<p>WEP:</p> <ul style="list-style-type: none"> • Wykorzystuje koder strumieniowy RC4, co jest kłopotliwym wyborem przy szyfrowaniu transmisji podzielonej na bloki danych zawarte w ramach transmisji bezprzewodowych. • Wykorzystuje 24-bitowy wektor inicjalizacyjny oraz 40 lub 104-bitowy klucz tajny. Po prostym połączeniu tych elementów tworzony jest klucz szyfrujący wykorzystywany przez algorytm RC4. • Klucz szyfrujący jest używany zarówno do uwierzytelniania użytkowników, jak i do ochrony poufności. • Brak jest kryptograficznej ochrony integralności – zastosowano jedynie funkcję kontroli parzystości CRC. <p>WPA:</p> <ul style="list-style-type: none"> • Wykorzystuje koder blokowy AES. Jest to wybór lepszy niż użycie kodera strumieniowego, ze względu na fakt, iż transmitowane dane podzielone są na bloki zawarte w ramach transmisji bezprzewodowych. • W celu uwierzytelniania wykorzystywane jest hasło (8-64 bajtów) wspólne dla wszystkich użytkowników. • Hasło to nie jest używane do ochrony poufności lub integralności ruchu sieciowego. W tym celu wykorzystuje się 48-bitowy wektor inicjalizacyjny oraz losowo generowany przez urządzenia klucz tajny, które to elementy łączone są za pomocą specjalnej funkcji mieszającej tworząc klucz szyfrujący. • Klucz szyfrujący może być automatycznie, okresowo zmieniany. • Poufność ruchu chroniona jest z użyciem kodera AES pracującego w trybie Counter (CTR). • Integralność ruchu chroniona jest również z użyciem kodera AES lecz pracującego w trybie Cipher Block Chaining (CBC).
4.		<p>Na rys. 2 zaprezentowano wybrane elementy architektury systemu IP Multimedia Subsystem (niepełny schemat elementów funkcjonalnych oraz punktów styku pomiędzy nimi). Uzupełnij nazwy elementów funkcjonalnych oraz podaj nazwy protokołów wykorzystywanych dla punktów styku pogrupowanych kolorami czarnym, zielonym i pomarańczowym. (Dla uproszczenia w poniższym schemacie pominięto szereg elementów funkcjonalnych i punktów styku).</p>



Rys. 2. Wybrane elementy architektury systemu IP Multimedia Subsystem

Odpowiedź

Zielony: Diameter
 Czarny: SIP (Session Initiation Protocol)
 Pomarańczowy: RTP (Real-time Transport Protocol) lub SRTP (Secure Real-time Transport Protocol)
 1: HSS (Home Subscriber Server)
 2: P-CSCF (Proxy- Call Session Control Function)
 3: MRFP (Media Resource Function Processor) \

5. Dysponując pulą adresów IP 192.168.0.0/24 zaproponuj optymalny z punktu widzenia wykorzystania adresów IP plan adresacji dla 4 podsieci po 15 urządzeń. Wyznacz zagregowany adres routinowy i jego maskę dla zaproponowanego rozwiązania. W każdej podsieci należy przewidzieć 1 adres dla routera. Ile adresów IP pozostanie wolnych?

Odpowiedź

15 urządzeń + 1 adres dla routera wymusza minimalną maskę /27, w której jest $2^{(32-27)} - 2 = 2^5 - 2 = 30$ adresów użytecznych.

Plan adresacji:

- 1 podsieć 192.168.0.0/27
- 2 podsieć 192.168.0.32/27
- 3 podsieć 192.168.0.64/27
- 4 podsieć 192.168.0.96/27

W każdej podsieci jest $30 - 15 - 1 = 14$ wolnych adresów.

Łącznie wolnych pozostaje $4 * 14 = 56$ adresów IP.

Adres routinowy całej sieci to 192.168.0.0/25 obejmuje on wszystkie adresy we wszystkich 4 podsieciach.

6. Ogar przenosi paczkę zapelnionych 10 płyt DVD (płyty o pojemności 4,7 gigabajtów każda) między dwoma firmami oddalonymi od siebie o 1500 metrów. Ogar porusza się z

prędkością 12 km/ godz. Czy czas dostarczenia przez ogara danych zgromadzonych na płytach DVD będzie:

- wielokrotnie dłuższy
- nieco dłuższy
- nieco krótszy
- wielokrotnie krótszy

od czasu transmisji tych danych przez zbudowaną na światłowodach sieć GigabitEthernet, łączącą te firmy ?

Wskaż jak czynniki protokolarne (struktura ramek Ethernet) oraz czas propagacji wpływają na oszacowanie czasu przesyłania danych przez sieć GigabitEthernet.

Odpowiedź

Wolumen danych do przesłania:
 $W = 10 \text{ (sztuk DVD)} * 4,7 \text{ GB (gigabajtów)} * 8 \text{ (bitów)} = 376 \text{ Gb} = 376\,000\,000\,000 \text{ b}$

Czas transportu danych przez psa:
 $t = d/v = 1500 \text{ m} / 12 \text{ km/h} = 1500 \text{ m} / 3,333 \text{ m/s} = \mathbf{450 \text{ [s]}}$

Czas (oszacowanie – bez uwzględnienia czasu propagacji, struktury ramek ethernetowych) transportu danych przez sieć :
 $t = W \text{ [b]} / 1\,000\,000\,000 \text{ [b/s]} = 376\,000\,000\,000 \text{ [b]} / 1\,000\,000\,000 \text{ [b/s]} = \mathbf{376 \text{ [s]}}$

Czynniki które powodują, że oszacowanie czasu przesyłania danych przez sieć GigabitEthernet może być zaniżone

- czasu propagacji T_p
 $T_p = 1500 \text{ [m]} / 3 * 100\,000\,000 \text{ [m/s]} = 5 \text{ [ms]} \ll 376 \text{ s}$ (pomijalnie mały czas)
- w Ethernetie transfer danych jest realizowany poprzez podział całego wolumenu danych na fragmenty (ramki); każda ramka zawiera co najmniej 18 bajtów protokolarnych (6 -adres do kogo; 6 -adres od kogo; 2 -protokół; 4 - suma kontrolna);

Uwzględniając, że transfer ramek może odbywać ramkami o polu danych od 46 do 1500 bajtów (minimalna długość ramki 64 bajty; maksymalna długość ramki 1518 bajtów) efektywny transfer wynosi:

- jeżeli transport ramek jest realizowany przez wysyłanie ramek o minimalnej długości 64 bajtów, to efektywne wykorzystanie łączy jest rzędu $(64-6-6-2-4)/64$ (64bajty (całkowita długość ramki) – 6 (adres do kogo) -6 (adres od kogo), -2 (protokół), -4 (suma kontrolna)) / 64 = $46/64 = 72\%$; zatem
 $t = W \text{ [b]} / (0,72 * 1\,000\,000\,000 \text{ [b/s]}) = 376\,000\,000\,000 \text{ [b]} / (0,72 * 1\,000\,000\,000 \text{ [b/s]}) = \mathbf{523 \text{ [s]}}$
- jeżeli transport ramek jest realizowany przez wysyłanie ramek o maksymalnej długości 1518 bajtów, to wykorzystanie łączy jest rzędu $(1518-8-8-2-4)/64$ (1518bajty (całkowita długość ramki) – 6 (adres do kogo) -6 (adres od kogo), 2 (protokół), 4 (suma kontrolna)) / 1518 = $1500/1518 = 99\%$
 $t = W \text{ [b]} / (0,99 * 1\,000\,000\,000 \text{ [b/s]}) = 376\,000\,000\,000 \text{ [b]} / (0,99 * 1\,000\,000\,000 \text{ [b/s]}) = \mathbf{380 \text{ [s]}}$

Zatem prawidłowa odpowiedź to:
Czas dostarczenia przez ogara danych zgromadzonych na płytach DVD będzie nieco dłuższy (**450 s > 380 s**) lub nieco krótszy (**450 s < 523 s**) w zależności od wielkości ramek ethernetowych, które wykorzystamy do transferu danych.

<i>Opracowali:</i> mgr inż. Kanstantsin Myslitski dr inż. Tomasz Gierszewski dr inż. Krzysztof Gierłowski mgr inż. Michał Hoeft dr inż. Wojciech Gumiński dr inż. Krzysztof Nowicki dr hab. inż. Jacek Rak, prof. nadzw. PG	<i>Sprawdził:</i> dr inż. Jacek Majewski	<i>Zatwierdził:</i> Przewodniczący Rady Naukowej Olimpiady dr hab. inż. Sławomir Cieślik
---	--	---