

Wiązka zadań *Smartfon*

Rozważmy następujące aplikacje:

- serwis pogodowy,
- katalog książek biblioteki szkolnej,
- elektroniczny dziennik lekcyjny,
- edytor tekstu,
- serwis informacji turystycznej Wrocławia,
- wyszukiwanie optymalnej trasy samochodowej,
- arkusz kalkulacyjny,
- kompilator języka programowania,
- system komputerowego składu tekstu.

43.1.

Wskaż wśród powyższych aplikacji dwie, dla których przydatna jest informacja o położeniu geograficznym użytkowników korzystających z urządzeń mobilnych (np. smartfonów). Dla każdej z wybranych aplikacji opis w jednym lub dwóch zdaniach sposób wykorzystania danych o lokalizacji użytkowników.

Najpierw wskażmy aplikacje, dla których wykorzystanie informacji o położeniu geograficznym („lokalizacji”) jest przydatne w sposób oczywisty:

- *Serwis pogodowy: informacja o położeniu daje możliwość automatycznego wyboru prognozy pogody dla aktualnej lokalizacji użytkownika.*
- *Serwis informacji turystycznej Wrocławia: informacja o aktualnej lokalizacji użytkownika pomoże ustalić najbliższe atrakcje turystyczne oraz wskazać drogę do wybranych atrakcji.*
- *Wyszukiwanie optymalnej trasy samochodowej: to najlepiej znane zastosowanie systemów lokalizacji geograficznej; występuje w nim swoiste sprzężenie zwrotne: system wskazuje użytkownikowi optymalną drogę do celu, a jednocześnie dane o położeniu użytkowników pozwalają oszacować natężenie ruchu, co z kolei pozwala wybierać drogę omijającą tzw. korki samochodowe.*

Można wyobrazić sobie zastosowania lokalizacji w innych aplikacjach, np.:

- *Znajomość lokalizacji pozwoli zasugerować język używany w edytorze tekstu czy systemie komputerowego składu tekstu (np. w Polsce spodziewamy się korzystania z języka polskiego, a w Argentynie z języka hiszpańskiego).*
- *Lokalizacja pozwala zasugerować format danych w arkuszu kalkulacyjnym (np. format walutowy czy sposób prezentacji daty dopasowany do kraju). Nietrudno jednak wskazać wady i ograniczoną przydatność powyższych funkcjonalności. Personalizacja urządzeń mobilnych powoduje, że używany w edytorze tekstu język raczej przypisujemy do użytkownika, a nie do kraju, w którym on się znajduje. Wydaje się więc, że trudno o przekonujące argumenty na rzecz istotnej przydatności lokalizacji w edytorze tekstu, systemie komputerowego składu tekstu lub arkuszu kalkulacyjnym. Lokalizacja nie wydaje się też przydatna przy korzystaniu z katalogu książek biblioteki szkolnej. (Mogłaby być przydatna w przypadku biblioteki miejskiej czy uczelniowej: instytucje takie mają wiele oddziałów i aplikacja mogłaby znaleźć najbliższy oddział, w którym dostępna jest poszukiwana książka.) Trudno też wyobrazić sobie istotne zastosowania lokalizacji w elektronicznym dzienniku lekcyjnym lub kompilatorze języka programowania.*

Przykładowa odpowiedź:

- *Wyszukiwanie optymalnej trasy samochodowej*

Uzasadnienie: Dzięki lokalizacji znane jest położenie użytkownika co daje możliwość podawania wskazówek odnośnie wyboru drogi, dopasowanych do jego położenia oraz zmiany trasy, w przypadku informacji o korkach. Dane o lokalizacji użytkowników pozwalają oszacować natężenie ruchu na różnych odcinkach dróg

- *Serwis pogodowy*

Uzasadnienie: Dzięki usłudze lokalizacji użytkownicy mogą uzyskiwać dane pogodowe i prognozę pogody dla ich aktualnego położenia bez konieczności podawania lokalizacji samemu

- *Serwis informacji turystycznej Wrocławia*

Uzasadnienie: Wykorzystując dane o lokalizacji użytkownika, serwis może podać, jakie obiekty znajdują się najbliżej jego aktualnego położenia, a także wskazać trasę od miejsca, w którym użytkownik się aktualnie znajduje, do wybranego obiektu

43.2.

Wskaż wśród powyższych aplikacji co najmniej dwie, których przydatność jest istotnie ograniczona w sytuacji, gdy użytkownik ma jedynie dostęp do urządzenia mobilnego (np. smart fon, tablet). Dla każdej z wybranych aplikacji uzasadnij swój wybór w co najwyżej dwóch zdaniach.

Urządzenia mobilne typu smartfon/tablet są wygodne przede wszystkim w sytuacjach, w których użytkownik „konsumuje” treści (czyta, słucha). Brak dużej ergonomicznej klawiatury oraz odpowiednio dużego monitora zazwyczaj utrudnia tworzenie treści (pisanie tekstów, obsługę systemów składu tekstu, projektowanie CAD/CAM, pisanie i testowanie programów komputerowych, edycję zestawień w arkuszu kalkulacyjnym itp.). Uwzględniając powyższe czynniki, do aplikacji (z podanej listy), których przydatność jest istotnie ograniczona w sytuacji, gdy użytkownik ma jedynie dostęp do urządzenia mobilnego, zaliczyć można: system komputerowego składu tekstu, edytor tekstu, arkusz kalkulacyjny, kompilator języka programowania.

Przykładowa odpowiedź:

- System komputerowego składu tekstu

Uzasadnienie: Edycja wielu elementów (tekst + grafika) wymaga wprowadzania wielu danych (wpisywanie tekstu, wstawianie i tworzenie obiektów graficznych), a do tego celu przydatna jest ergonomiczna klawiatura, mysz itp. Wizualizacja w skali 1:1 wymaga odpowiednio dużego ekranu.

- Edytor tekstu

Uzasadnienie: Dużo ilość tekstu dużo wygodniej wprowadza się, korzystając z dużej, ergonomicznej klawiatury. Ponadto duży ekran umożliwia wizualizację wynikowego dokumentu w rzeczywistych wymiarach.

- Arkusz kalkulacyjny

Uzasadnienie: Dane (zestawienia liczbowe, teksty) i formuły wygodniej wprowadza się, korzystając z dużej, ergonomicznej klawiatury. Dotyczy to również tworzenia i przeglądania wykresów.

43.3.

Zdjęcia wykonywane na smartfonie Franka gromadzone są na jego koncie w chmurze obliczeniowej, o ile smartfon jest podłączony do Internetu. W przypadku braku dostępu do Internetu zdjęcia gromadzone są w pamięci podręcznej. Przy obecnych ustawieniach smartfonu często występuje problem braku miejsca w pamięci podręcznej, uniemożliwiający robienie dużej liczby zdjęć. Franek chciałby zmienić ustawienia tak, aby możliwe było zachowanie w pamięci większej liczby zdjęć.

Wśród podanych niżej sposobów wskaż te, które mogą pomóc w rozwiązaniu problemu Franka (zaznacz znakiem X która odpowiedź jest prawdziwa, a która jest fałszywa):

	P	F
zmiana formatu zapisu zdjęć na mapę bitową		X
zmniejszenie rozdzielczości zapisywanych zdjęć	X	
zastosowanie kodów korekcji CRC, opartych na bitach parzystości		X
obniżenie jakości kompresji zdjęć (w formacie JPEG)	X	

Mapa bitowa (np. format BMP) nie wykorzystuje zależności między pikselami, które pozwalają zmniejszać pamięć potrzebną do cyfrowej reprezentacji zdjęć. Z kolei zastosowanie kodów korekcji CRC służy zwiększeniu odporności na błędy zapisu, odczytu lub transmisji danych kosztem zwiększenia rozmiaru danych. Przez rozdzielczość zdjęcia rozumiemy liczbę wierszy oraz liczbę kolumn w tablicy pikseli, z których zdjęcie się składa. Zmniejszenie rozdzielczości oznacza zmniejszenie liczby kolumn i liczby wierszy w tej tablicy. Przy zdjęciach wysokiej jakości pozwala to znacznie ograniczyć rozmiar jego cyfrowej reprezentacji bez znacznej straty jakości zdjęcia. Celem kompresji jest zmniejszenie rozmiaru danych. Standard JPEG opisuje sposób kompresji obrazów. Jest powszechnie stosowany w cyfrowym zapisie zdjęć. W kompresji JPEG możemy zmniejszać rozmiar pliku kosztem pogorszenia wizualnej jakości zdjęcia (jakości kompresji). Podsumowując, prawdziwe jest zdanie drugie i czwarte, natomiast pierwsze i trzecie są fałszywe.

43.4.

Franek założył konto w banku i zamierza korzystać z bankowości internetowej. Wśród poniższych funkcjonalności wskaż te, które mogą służyć zabezpieczeniu usług bankowości internetowej przed nieuprawnionym dostępem (zaznacz znakiem X która odpowiedź jest prawdziwa, a która jest fałszywa):

	P	F
protokół transferu plików FTP (File Transfer Protocol).		X
protokół SSL (Secure Socket Layer).	X	
uwierzytelnianie użytkownika przy pomocy hasła lub PIN.	X	
kompresja dysku twardego.		X
hasła jednorazowe generowane przez układy kryptograficzne i dostarczane kanałami informacyjnymi alternatywnymi dla Internetu.	X	

Protokół FTP umożliwia przesyłanie plików poprzez sieć, nie zawiera jednak żadnych mechanizmów ochrony przed nieuprawnionym dostępem. Z kolei protokół SSL został zaprojektowany właśnie w celu umożliwienia transferu zapewniającego poufność i integralność przesyłanych danych, a także uwierzytelniania uczestników komunikacji (wykorzystuje się do tych celów odpowiednie mechanizmy kryptograficzne); narzędzia te są w szczególności przydatne przy korzystaniu z usług bankowości internetowej (patrz przedrostek https w adresie internetowym). Naturalnymi mechanizmami ochrony dostępu do indywidualnych kont są

również hasła i PINy. Ich wzmocnieniem są często hasła jednorazowe tworzone dla potwierdzenia pojedynczych operacji/czynności. Celem kompresji jest przede wszystkim zmniejszenie rozmiaru cyfrowej reprezentacji danych. Zazwyczaj nie wiąże się ono z ochroną prywatności, poufności bądź ochroną przed nieuprawnionym dostępem. Powyższe uwagi prowadzą do następującego rozwiązania zadania: FPPFP

Zadanie 44.

Zdecyduj, które z dokończeń podanego niżej zdania czynią z niego zdanie prawdziwe (P), a które fałszywe (F). Zaznacz to znakiem X w odpowiednich miejscach tabeli.

Liczba 1001100102

	P	F
jest dwa razy większa od liczby 100110012.	X	
jest dwa razy mniejsza od liczby 10011001002.	X	
jest większa niż 51210.		X
jest mniejsza niż 4728.	X	

$$100110010_2 = 1 \cdot 2^8 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^1 = 256 + 32 + 16 + 2 = 306.$$

Odpowiedź na pytanie pierwsze jest prawdziwa, ponieważ $100110012 = 1 \cdot 2^7 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^0 = 153$.

Odpowiedź na pytanie drugie jest prawdziwa, ponieważ $10011001002 = 1 \cdot 2^9 + 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^2 = 612$.

Odpowiedź na pytanie trzecie jest fałszywa, ponieważ liczba 306 jest mniejsza niż 512.

W przypadku odpowiedzi na czwarte pytanie można zamienić liczbę zapisaną w systemie ósemkowym na system dziesiętny: $472_8 = 4 \cdot 8^2 + 7 \cdot 8^1 + 2 \cdot 8^0 = 314$, zatem odpowiedź jest prawdziwa.

Zadanie 45.

Wskaż elementy, które są niezbędne do uruchomienia komputera i załadowania systemu operacyjnego.

	P	F
Procesor	X	
twardy dysk		X
pamięć operacyjna	X	
Monitor		X

Procesor jest centralną jednostką komputera, która wykonuje wszystkie obliczenia i steruje wykonywaniem instrukcji. Komputer nie może działać bez procesora. Pamięć operacyjna jest konieczna, aby przechowywać dane, w tym podstawową część (jądro) systemu operacyjnego — komputer bez pamięci nie jest w stanie działać.

Komputer może działać bez twardego dysku: możliwe jest uruchomienie systemu operacyjnego z płyty CD lub pamięci typu flash, a nawet przez sieć lokalną, przy zdalnym użyciu dysku znajdującego się w innym komputerze.

Komputer może bez żadnych przeszkód działać bez monitora. Często na przykład w ten sposób pracują długo działające serwery, które wygodniej obsługiwać zdalnie, logując się na nie z innego komputera.

Zadanie 46.

Zaznacz znakiem X w odpowiedniej kolumnie, które zdanie jest prawdziwe, a które jest fałszywe.

	P	F
System operacyjny przydziela zadaniom czas pracy procesora.	X	
System operacyjny używa zawsze tego samego systemu plików dla wszystkich urządzeń.	X	
W skład systemu operacyjnego wchodzi zawsze graficzny interfejs użytkownika.		X
System operacyjny przydziela uruchamianym aplikacjom pamięć operacyjną.	X	

Do głównych zadań systemu operacyjnego należy:

- przydział poszczególnym zadaniom czasu procesora (odpowiedź P w pierwszym zdaniu);
- przydział poszczególnym zadaniom pamięci operacyjnej (odpowiedź P w czwartym zdaniu);
- dostarczenie mechanizmów synchronizacji zadań i komunikacji między nimi;
- obsługiwanie sprzętu oraz zapewnienie równoległym wykonywanym zadaniom oraz synchronizuje dostęp procesów do niego.

Dodatkowo system operacyjny może posiadać środowisko graficzne ułatwiające komunikację z użytkownikiem (w trzecim zadaniu właściwa jest odpowiedź F). Większość obecnie używanych systemów operacyjnych posiada graficzny interfejs użytkownika. Przykładami systemu operacyjnego bez środowiska graficznego są Microsoft DOS oraz GNU/Linux bez XWindows. Większość systemów operacyjnych posiada własny system plików, rozwijany równoległe z nim, ze względu na pewne specyficzne właściwości nadawane plikom (np. atrybut wykonywalności pliku). Z powodów użytkowych systemy operacyjne potrafią obsługiwać wiele systemów plików, w szczególności inny system do urządzeń wielokrotnego zapisu (w zależności do systemu operacyjnego może to być np. FAT/NTFS/ext3/HFS), a inny do płyt CD/DVD z ograniczonymi możliwościami ponownego zapisu, np. ISO9660 lub UDF (w drugim zadaniu właściwa jest odpowiedź F).

Zadanie 47.

Zaznacz znakiem X w odpowiedniej kolumnie, które zdanie jest prawdziwe (P), a które jest fałszywe (F).

System plików NTFS

	P	F
nie jest obsługiwany przez system Linux.		X
przechowuje informację o rozmiarze, dacie utworzenia i modyfikacji pliku oraz o ścieżce dostępu do pliku.	X	
uniemożliwia zapisanie pojedynczego pliku o rozmiarze powyżej 4 GB.		X
umożliwia administratorowi nadawanie pojedynczym użytkownikom lub grupom użytkowników praw dostępu do plików i katalogów.	X	

NTFS to standardowy system plików poczynsany od systemu Windows NT, poprzez jego kolejnych następców, aż do Windows 7 i Windows 8. Dla Linuxa to system plików obcego pochodzenia, ale po zainstalowaniu odpowiedniego sterownika Linux potrafi go obsługiwać. NTFS przechowuje informację o rozmiarze, dacie utworzenia i modyfikacji pliku oraz ścieżce dostępu do pliku. NTFS nie ogranicza maksymalnego rozmiaru pliku do 4GB w przeciwieństwie do FAT32. W NTFS funkcjonuje tzw. lista kontroli dostępu (ACL), która umożliwia administratorowi nadawanie praw dostępu do plików i katalogów pojedynczym użytkownikom lub grupom użytkowników.

Zadanie 48.

Zaznacz znakiem X w odpowiedniej kolumnie, które zdanie jest prawdziwe, a które jest fałszywe.

W pewnej firmie znajdują się m.in. komputery o następujących adresach IP:

- komputer A: 10.20.30.40 / maska 255.255.0.0; 10.x.x.x 192.168.x.x 172.168.x.x
- komputer B: 10.0.0.10 / maska 255.255.255.0;
- komputer C: 1.2.3.4 / maska 255.255.255.0;
- komputer D: 1.2.3.250 / maska 255.255.255.0.

	P	F
Komputer A może być widoczny w sieci Internet pod innym adresem IP.	X	
Tylko dwa z wymienionych komputerów mogą mieć dostęp do sieci Internet.		X
Komputery A i B znajdują się w jednej podsieci.		X
Komputery C i D muszą znajdować się w jednym budynku.		X

Dla poprawnego udzielenia odpowiedzi trzeba ustalić adresy sieci, w których położone są cztery komputery.

Na podstawie adresu IP i maski sieciowej można ustalić, że adresy te to:

- w przypadku komputera A: 10.20.0.0 / maska 255.255.0.0, w skrócie 10.20.0.0/16;
- w przypadku komputera B: 10.0.0.0 / maska 255.255.255.0; w skrócie 10.0.0.0/24;
- w przypadku komputera C: 1.2.3.0 / maska 255.255.255.0; w skrócie 1.2.3.0/24;
- w przypadku komputera D: 1.2.3.0 / maska 255.255.255.0; w skrócie 1.2.3.0/24.

Zdanie 1: Komputer A używa adresu IP z puli tzw. adresów prywatnych, a więc niedostępnych z sieci Internet. Komputer ten musi być podłączony do sieci Internet za pośrednictwem routera, który przy okazji może też przekierowywać ruch adresowany do pewnego publicznego adresu IP na ten właśnie komputer. (Zdanie jest prawdziwe).

Zdanie 2: Dwa z czterech komputerów używają adresów prywatnych, dwa — adresów publicznych. Nie ma to jednak znaczenia w przypadku dostępu do sieci Internet. Wszystkie wymienione komputery, niezależnie od adresu IP, jaki mają przypisany w sieciach lokalnych, mogą mieć dostęp do sieci Internet. (Zdanie jest fałszywe).

Zdanie 3: Komputer A jest w podsieci 10.20.0.0/16, a komputer B — w podsieci 10.0.0.0/24. Leżą zatem w różnych podsieciach. (Zdanie jest fałszywe).

Zdanie 4: Komputery C i D mają takie same adresy sieci (1.2.3.0/24) i są one publiczne, więc jest to ta sama podsieć. Nie ma to jednak znaczenia dla fizycznego położenia tych komputerów w jednym budynku, mogą się one znajdować w różnych budynkach. (Zdanie jest fałszywe)

Zadanie 49.

Chmura obliczeniowa jest usługą polegającą na zdalnym udostępnieniu mocy obliczeniowej urządzeń IT, oferowaną przez zewnętrznego dostawcę. Oceń prawdziwość poniższych zdań, umieszczając znak X w odpowiedniej kolumnie tabeli.

		P	F
A	Z aplikacji i danych umieszczonych w chmurze można korzystać z dowolnej lokalizacji i dowolnego sprzętu IT umożliwiającego połączenie internetowe.	X	
B	Użytkownik nie jest zobowiązany do zakupu licencji na oprogramowanie używane w chmurze i udostępniane przez dostawcę, płaci jedynie za jego użycie (každorazowo lub w formie abonamentu).	X	
C	Użytkownik może zdalnie instalować w przydzielonych zasobach chmury dowolne aplikacje i korzystać z nich tak jak na lokalnym komputerze.		X
D	Pula zasobów użytkownika (w tym: procesory, pamięć RAM, przestrzeń dyskowa) jest elastycznie skalowana w zależności od jego potrzeb i ograniczona tylko możliwościami dostawcy.	X	

Zasada działania chmury obliczeniowej polega na przeniesieniu całego ciężaru świadczenia usług IT (danych, oprogramowania, mocy obliczeniowej) na serwer

i umożliwienie stałego dostępu do niego komputerom klientów. Wystarczy zalogować się z jakiegokolwiek komputera z dostępem do Internetu, by zacząć korzystać z chmury obliczeniowej. Chmura obliczeniowa jest szerokim pojęciem, zmierzającym w takim kierunku, aby całe oprogramowanie było instalowane na serwerze, zaś w komputerze klienta znajdował się tylko interfejs do komunikacji z tym oprogramowaniem. Oprogramowanie nie jest kopiowane i powielane w komputerze klienta, więc klient nie narusza praw autorskich i nie musi wykupować licencji, płaci jedynie za użytkowanie programów. Klient nie instaluje oprogramowania na serwerze. Dokumenty i dane klienta przechowywane są na serwerze, na ich bezpieczeństwo nie mają wpływu ewentualne awarie komputera klienta. Szybkość obliczeń zależy od mocy obliczeniowej serwera. Moc obliczeniowa (procesory, pamięć RAM, przestrzeń dyskowa, przepustowość łącza internetowego itp.) może być zwiększana lub zmniejszana na życzenie klienta, jest ograniczona tylko wielkością zasobów usługodawcy. Opłaty naliczane są za faktycznie wykorzystaną moc obliczeniową w danym czasie.

Zadanie 50.

HTTP Cookie jest niewielką porcją informacji wysyłaną przez witrynę internetową do przeglądarki klienta i zapisywaną w jej ustawieniach. Oceń prawdziwość poniższych zdań, umieszczając znak X w odpowiedniej kolumnie tabeli.

		P	F
A	Cookie zawiera polecenia, które konfiguruja ustawienia przeglądarki klienta.		X
B	Cookie umożliwia serwisowi sprawdzenie, czy klient już go odwiedzał w przeszłości, oraz zapamiętanie upodobań klienta.	X	
C	Cookie zapisane przez serwis z domeny cwaniak.org może być odczytane przez serwis z domeny spryciarz.org.		X
D	Zablokowanie obsługi cookie w przeglądarce może spowodować utrudnienia dla użytkownika dokonującego zakupów w sklepie internetowym.	X	

HTTP Cookie jest krótkim tekstem (o rozmiarze maksymalnie 4 kB), który serwer witryny internetowej wysyła do przeglądarki klienta. Przy następnych odwiedzinach tej witryny przez klienta serwer próbuje odczytać swoje cookie. Odczyt cookie przez serwer jest możliwy tylko z domeny, która ustawiła to cookie, lub z jej subdomeny. Cookie może mieć ustawiony czas życia, tzn. czas przechowywania w ustawieniach przeglądarki. Jeśli nie ma ustawionego czasu życia, jest przechowywane tylko do chwili zamknięcia okna przeglądarki. W treści cookie może być zawarta informacja o preferencjach klienta: jego różnych wyborach podczas odwiedzin witryny. Z poziomu cookie nie ma możliwości wykonania poleceń, w szczególności dotyczących konfiguracji przeglądarki. Przeglądarki umożliwiają kontrolę zapisanych http cookie (przeglądanie, usuwanie) oraz zablokowanie samej obsługi cookie. Witryny sklepów internetowych ustawiają HTTP cookie po zalogowaniu klienta (zapisują identyfikator sesji), aby rozpoznać tego klienta, gdy przechodzi on między różnymi stronami serwisu sklepowego, wybierając towary do koszyka. Zablokowanie obsługi cookie w przeglądarce może uniemożliwić serwisowi opartemu na mechanizmie sesji rozpoznanie klienta i skompletowanie jego koszyka.

Uwaga: Istnieje także inny rodzaj cookie: Flash Cookies, znane jako Local Shared Objects, zapisywane przez przeglądarkę internetową (dokładniej: przez plugin Flash) po wejściu na stronę WWW zawierającą obiekt Flash, np. banner. Zawierają one także tekst, ale mogą osiągać rozmiar do 100 kB, nie mają określonego czasu wygaśnięcia (nie są automatycznie usuwane) i nie można ich przeglądać ani usunąć z poziomu ustawień przeglądarki. Można jedynie ustawić rozmiar przechowywanych danych w ustawieniach Adobe Flash Playera.

Zadanie 51.

Czterech użytkowników założyło konta w pewnym serwisie internetowym. Wybrali następujące dane logowania:

Użytkownik A	nazwa użytkownika: <i>jankowalski</i> hasło: <i>1234</i>
Użytkownik B	nazwa użytkownika: <i>merkuriusz 312</i> hasło: <i>merkuriusz 312</i>
Użytkownik C	nazwa użytkownika: <i>abc</i> hasło: <i>S4o9s2n5a7</i>
Użytkownik D	nazwa użytkownika: <i>master</i> hasło: <i>password</i>

Przestępca usiłuje przejąć konta użytkowników, stosując w tym celu następujące dwie techniki:

- atak *bruteforce* (wszystkie możliwe kombinacje znaków),
- metoda psychologiczna i słownikowa (zgadnięcie hasła, sprawdzenie popularnych haseł i słów).

Wskaż, które hasła są podatne na złamanie tymi metodami, stawiając w odpowiednim polu tabeli znak X, jeśli taka podatność występuje:

	atak <i>brute force</i>	metoda słownikowa/psychologiczna
Użytkownik A	X	
Użytkownik B		X
Użytkownik C		X
Użytkownik D		X

Metoda brute force działa tylko na krótkich hasłach, najlepiej na takich, które złożone są z samych liter lub samych cyfr („1234”, „axf”).

Na atak słownikowy podatne są wszystkie hasła, które są trywialnymi ciągami kolejnych liter lub cyfr („abcdef”, „1234”, ale również kolejne litery na klawiaturze: „qwerty”), hasła będące prostymi słowami, zwłaszcza kojarzącymi się z hasłem („hasło”, „password”, „Ania”, „komputer”, „admin”), a także hasło identyczne z nazwą użytkownika.

Zadanie 52.

Zaznacz znakiem X w odpowiedniej kolumnie, które zdanie jest prawdziwe (P), a które jest fałszywe (F).

W grafice rastrowej 24bitowe kodowanie koloru oznacza, że

	P	F
liczba kolorów w palecie barw wynosi ponad 16 milionów.	X	
informacje o kolorze jednego piksela zajmują 3 bajty.	X	
liczba kolorów jest niewystarczająca do zapisu zdjęć.		X
obraz o rozmiarach 300x300 pikseli zapisany bez kompresji ma wielkość około 2,16 MB.		X

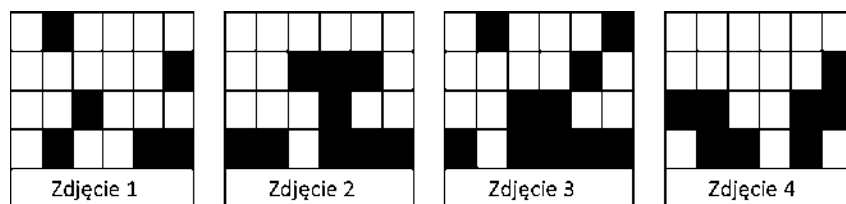
24-bitowy kolor oznacza, że na opis koloru pojedynczego piksela przeznaczają się 24 bity, co oznacza, że mamy do dyspozycji paletę barw o $2^{24} = 16\,777\,216$ kolorów. 24 bity to 3 bajty. Oko człowieka nie dostrzega różnicy pomiędzy obrazem rzeczywistym a zapisanym przy pomocy 24-bitowej palety barw, dlatego taką paletę nazywa się true colour i stosuje się do zapisu fotografii.

W przypadku obrazów rastrowych o rozdzielczości 300x300 pikseli mamy 90 000 pikseli opisanych przez 24 bity każdy. $90\,000 \cdot 24 \text{ bity} = 2\,160\,000 \text{ bitów} = 270\,000 \text{ bajtów} = 270 \text{ KB}$.

Zadanie 53.

Wiązka zadań Zegar binarny

Pan Kowalski postanowił wyjechać na wycieczkę na wyspę Binarną. Mieszkańcy tej wyspy do zapisywania cyfr dziesiętnych używają metody obrazkowej, opartej na systemie binarnym. Podczas pobytu na wyspie Pan Kowalski wybrał się na jednodniową wycieczkę objazdową. W jej trakcie zrobił 4 poniższe zdjęcia zegara używanego na wyspie. Stan zegara podawany jest w formacie GG:MM:SS, gdzie GG to godzina, MM to minuty, a SS to sekundy (zapisane zawsze przy pomocy dwóch cyfr). Każda cyfra zapisana jest w osobnej kolumnie.



Pierwsze zdjęcie zostało zrobione w momencie rozpoczęcia wycieczki, ostatnie zdjęcie — w chwili jej zakończenia, zdjęcia 2 i 3 zostały natomiast zrobione w trakcie wycieczki.

53.1.

Podaj w systemie dziesiętnym stany zegara wyświetlane na zdjęciach 1 oraz 4.

Stan zegara na zdjęciu nr 1: 9:20:15 (09:20:15).

Stan zegara na zdjęciu nr 4: 23:10:36

Na początku na podstawie zawartości zdjęć chcemy ustalić, jak w zegarze kodowane są bity 0 i 1 (który z nich kodowany jest białym kolorem, a który — czarnym), a także, czy liczby w kolumnach kodowane są „od góry do dołu” (najbardziej znaczący bit jest najwyżej, naj-mniej znaczący najniżej), czy też odwrotnie. Z treści zadania wynika, że wyświetlane „metodą obrazkową” na kolejnych zdjęciach stany zegara oznaczają coraz późniejszą porę. W szczególności na zdjęciu 1 wartość godziny jest najmniejsza, a na zdjęciu 4 — największa. Przeanalizujmy kolumny z godzinami na czterech zdjęciach. Na pierwszym zdjęciu w pierwszej kolumnie występują tylko białe komórki, zatem biały kolor oznacza bit 0 (w przeciwnym razie pierwsza cyfra godziny byłaby równa 15, co oznacza kodowanie godziny niezgodne z przyjętym opisem). Na drugim i trzecim zdjęciu czarna jest pierwsza komórka od dołu w pierwszej kolumnie, zatem możemy rozważyć dwa sposoby kodowania: od góry (0001) i od dołu (1000). Wartość dziesiętna pierwszego zapisu wynosi 1, drugiego 8. Poprawnym wynikiem jest 1, gdyż pierwszą cyfrą godziny w układzie GG może być tylko 0, 1, 2. Zatem zapis binarny poszczególnych cyfr na zegarze ma najbardziej znaczący bit w pierwszym wierszu od góry.

Stąd łatwo odczytać godziny na kolejnych zdjęciach:

Zdjęcie 1 — 09:20:15

Zdjęcie 2 — 11:47:51

Zdjęcie 3 — 18:33:59

Zdjęcie 4 — 23:10:36

53.2.

Pan Kowalski położył się spać o godzinie 23:45:29. Zamaluj odpowiednie pola poniższej planszy tak, aby reprezentowała ona tę godzinę na zegarze używanym przez mieszkańców wyspy.

Aby zamalować w drugim zadaniu odpowiednie pola, musimy zamienić zapis poszczególnych cyfr z systemu dziesiętnego na binarny (możemy także wykorzystać informacje o sposobie kodowania z pierwszego zadania):

$$2_{(10)} = 0010_{(2)}$$

$$3_{(10)} = 0011_{(2)}$$

$$4_{(10)} = 0100_{(2)}$$

$$5_{(10)} = 0101_{(2)}$$

$$2_{(10)} = 0010_{(2)}$$

$$9_{(10)} = 1001_{(2)}$$

Przepisując zapis binarny (w ustalonym powyżej porządku) do planszy zegara, otrzymujemy:

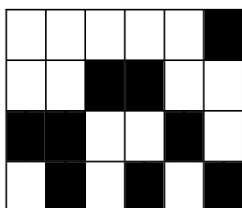
000001

001100

110010

010101

Następnie zamieniając 1 na czarne pola, zaś 0 na pola białe, otrzymujemy rozwiązanie zadania:



Zadanie 54.

Zaznacz znakiem X w odpowiedniej kolumnie, które zdanie jest prawdziwe (P), a które jest fałszywe (F).

Stos jest strukturą danych, która umożliwia

	P	F
bezpośredni dostęp do ostatnio zapisanego elementu.	X	
bezpośredni dostęp do każdego elementu stosu.		X
bezpośredni dostęp do najmniejszego i największego elementu stosu.		X
dodanie nowego elementu oraz usunięcie najpóźniej dodanego elementu.	X	

Stos jest liniową strukturą danych, w której są one dokładane na wierzch stosu i z wierzchołka stosu pobierane. Mamy możliwość dodania nowego elementu, bezpośredni dostęp do ostatnio zapisanego elementu oraz możliwość usunięcia najpóźniej dodanego elementu.

Zadanie 55.

Wiązka zadań *Zadania Zamknięte Funkcja*

Dana jest następujący algorytm $F(n)$ dla $n \in N, n > 0$

$F(n)$

jeżeli $n = 1$, zwróć 1 i zakończ w przeciwnym razie
zwróć $F(n \text{ div } 2) + 1$

55.1.

Złożoność tego algorytmu jest

	P	F
wykładnicza.		X
logarytmiczna.	X	
liniowa.		X
kwadratowa.		X

Należy zauważyć, że w każdym wywołaniu funkcji $F(n)$ argument jest zmniejszany dwukrotnie. Pytanie o złożoność można zamienić na pytanie: Ile razy należy dzielić n na pół, aby uzyskać $n = 1$?

Dla $n = 8 = 2^3$ kolejne wywołania funkcji to $F(4)$, $F(2)$, $F(1)$, czyli dzielenie występuje 3 razy.

Dla $n = 16 = 2^4$ kolejne wywołania to $F(8)$, $F(4)$, $F(2)$, $F(1)$, czyli dzielenie występuje 4 razy.

Dla $n = 2^k$ takie dzielenie będzie występowało k razy, zatem złożoność algorytmu jest logarytmiczna

55.2.

Dla tego algorytmu zachodzi

	P	F
$F(8) = 3$.		X
$F(12) = 4$.	X	
$F(1) = 0$ lub $F(9) = 4$.	X	
$F(1) = 1$ oraz $F(9) = 3$.		X

Zadanie można rozwiązać na 2 sposoby. Można przeanalizować działanie funkcji F dla podanych argumentów, np.

$F(8)=F(4)+1=(F(2)+1)+1=((F(1)+1)+1)+1=((1+1)+1)+1=4$;

$$F(12)=F(6)+1=(F(3)+1)+1=((F(1)+1)+1)+1=((1+1)+1)+1=4.$$

Można też zauważyć, że funkcja F oblicza liczbę bitów potrzebnych do zapamiętania liczby n w systemie binarnym; w ten sposób zadanie bardzo się upraszcza.

I tak do zapamiętania $n = 8$, $n = 9$, $n = 12$ potrzebujemy 4 bitów, a dla $n = 1$ potrzebujemy 1 bitu. Stąd łatwo uzyskujemy dwie pierwsze odpowiedzi.

Przy udzielaniu odpowiedzi na kolejne pytania trzeba pamiętać o tym, że wartość wyrażenia a lub b jest fałszywa tylko w wypadku, gdy zarówno $a = \text{fałsz}$, jak i $b = \text{fałsz}$ (w pozostałych przypadkach jest prawdziwa), zaś wartość wyrażenia a oraz b jest prawdziwa tylko wtedy, gdy zarówno $a = \text{prawda}$, jak i $b = \text{prawda}$ (w pozostałych przypadkach jest fałszywa).

Stąd otrzymamy:

$F(1) = 0$ lub $F(9) = 4 \Leftrightarrow \text{fałsz lub prawda} \Leftrightarrow \text{prawda}$,

$F(1) = 1$ oraz $F(9) = 3 \Leftrightarrow \text{prawda oraz fałsz} \Leftrightarrow \text{fałsz}$.

Zadanie 56.

Piractwo komputerowe jest przestępstwem polegającym na:

	P	F
wykorzystywaniu oprogramowania w celu osiągnięcia korzyści majątkowej, bez licencji na jego użytkowanie.	X	
instalowaniu wersji demo oprogramowania, którego licencję planujemy kupić.		X
rozpowszechnianiu w Internecie programów komputerowych, których licencję zakupiliśmy.	X	
oferowaniu za darmo w Internecie oprogramowania rozpowszechnianego na licencji freeware.		X

Aby zgodnie z prawem korzystać z programu komputerowego, powinniśmy posiadać licencję na jego użytkowanie. W przeciwnym razie dopuszczamy się kradzieży, a odpowiedzialność za tego typu czyn przewiduje art. 278 par. 1 kk, który mówi: "Kto zabiera w celu przywłaszczenia cudzą rzecz ruchomą podlega karze pozbawienia wolności od 3 miesięcy do 5 lat". A w odniesieniu do programu komputerowego par. 2 tegoż art. stwierdza: "Tej samej karze podlega, kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowej". Warunki licencji na użytkowanie programu precyzują, co można zrobić z posiadanym programem. Zazwyczaj licencje płatne nie dopuszczają odstępowania programu innym osobom. Warunki licencji freeware dopuszczają rozpowszechnianie programu, ale bez możliwości czerpania korzyści finansowych z tego tytułu. Wersje demo programów można z zasady instalować na komputerze, nie posiadając licencji na dany program. Celem udostępniania wersji demo jest zachęcenie (potencjalnego) klienta do zakupu licencji.

Zadanie 57.

Zgodnie z prawem w Internecie można opublikować zdjęcie osoby:

	P	F
po uzyskaniu od niej zezwolenia.	X	
gdy jest to osoba powszechnie znana i zdjęcie zostało wykonane podczas pełnienia przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych.	X	
gdy osoba ta jest naszym bliskim znajomym.		X
gdy stanowi ona jedynie szczegół całości takiej jak: zgromadzenie, krajobraz, publiczna impreza.	X	

Poprawne odpowiedzi do zadania wynikają bezpośrednio z treści zapisów Ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 1994 nr 24 poz. 83): „Rozdział 10 Ochrona wizerunku, adresata korespondencji i tajemnicy źródeł informacji Art. 81. 1. Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie.

2. Zezwolenia nie wymaga rozpowszechnianie wizerunku: osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych; 2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.”