

## Sieci komputerowe, ćwiczenie: Zasady bezpieczeństwa

1. Trzy kolejne etapy uzyskania dostępu do zasobów to:

- (a) identyfikacja,
- (b) uwierzytelnianie,
- (c) autoryzacja.

Wyjaśnij znaczenie tych pojęć.

2. Zwyczajowo dzieli się sposoby uwierzytelniania na trzy kategorie. Jakież?

3. Podaj jeden przykład każdej kategorii z poprzedniego pytania.

4. Równoczesne uwierzytelnianie i autoryzacje nazywamy? Podaj dwa przykłady.

5. Szyfrowanie chroni przed? (wymień dwie rzeczy)

6. Wyjaśnij różnice pomiędzy 'zwykłym' kluczem (kryptografia symetryczna) a kluczem publicznym i kluczem prywatnym przy wysyłaniu i odbieraniu zaszyfrowanych wiadomości (kryptografia asymetryczna).

7. Opisz zasady działania podpisów cyfrowych i jak one się różnią od wysyłania zaszyfrowanych wiadomości.

8. Do czego służą certyfikaty?