1. Vyberte zo zoznamu metódy pre zabezpečenie bezdrôtových sietí a zoraďte ich od najmenej bezpečnej (1) po najbezpečnejšiu (*x*).

\_\_\_ RSA (algoritmus Rivest Shamir Adleman)

\_\_\_ EAP (Extensible Authentication Protocol)

\_\_\_ WPA (Wi-Fi Protected Access)

\_\_\_ WEP (Wired Equivalent Privacy)

\_\_\_ TKIP (Temporary Key Integrity Protocol)

\_\_\_ DES (Data Encryption Standard)

\_\_\_ WPA2 (Wi-Fi Protected Access verze 2)

\_\_\_ AES (Advanced Ecryption Standard)

\_\_\_ PGP (Pretty Good Privacy)

\_\_\_ WEP2 (Wired Equivalent Privacy verze 2)

\_\_\_ IDS (Intrusion Dection System)

\_\_\_ TLS (Transport Layer Security)

1. Priraďte význačné vlastnosti jednotlivým technológiám.

|  |  |
| --- | --- |
| **WEP** | **WPA** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**1** – krátky kľúč

**2** – statický kľúč

**3** – technológia dočasného kľúča (tzv. dynamický kľúč)

**4** – použitie šifrovacieho algoritmu RC4

**5** – technológia rieši integritu dát z bezpečnostného hľadiska

**6** – technológia nerieši integritu dát z bezpečnostného hľadiska

**7** – výpočtovo náročný

**8** – výpočtovo nenáročný