1. Vyberte ze seznamu metody pro zabezpečení bezdrátových sítí a seřaďte je od nejméně bezpečné (1) po nejvíce bezpečné (*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. Přiraďte význačné vlastnosti jednotlivým technologiím.

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

**1** – krátký klíč

**2** – statický klíč

**3** – technologie dočasného klíče (tzv. dynamický klíč)

**4** – použití šifrovacího algoritmu RC4

**5** – technologie řeší integritu dat z bezpečnostního hlediska

**6** – technologie neřeší integritu dat z bezpečnostního hlediska

**7** – výpočetně náročný

**8** – výpočetně nenáročný