RSA (Rivest-Shamir-Adleman)

RSA je kryptosystém s veřejným klíčem, který se stal základním kamenem bezpečnosti na internetu. Používá se pro dvě hlavní úlohy:

```
1. **Šifrování dat:** Aby zprávu mohl přečíst pouze zamýšlený příjemce.
2. **Digitální podpisy:** Aby bylo možné ověřit, že zprávu skutečně poslal daný odesílatel a nebyla cestou změněna.
```

Algoritmus byl zveřejněn v roce 1977 a jeho bezpečnost je založena na extrémní obtížnosti matematického problému: **faktorizace (rozkladu) velkých čísel**.

Jak RSA funguje (Princip klíčů)

RSA využívá asymetrický model, kde má každý uživatel dvojici klíčů:

- **Veřejný klíč (Public Key):** Může ho znát kdokoliv. Slouží k „uzamčení“ (zašifrování) zprávy.
- **Soukromý klíč (Private Key):** Musí zůstat v tajnosti. Slouží k „odemknutí“ (dešifrování) zprávy.

Matematické pozadí (Zjednodušeně):

```
1. Vyberou se dvě velmi velká prvočísla ($p$ a $q$).
2. Vynásobí se spolu, čímž vznikne číslo $n$ (modul).
3. Najít $p$ a $q$ jen na základě znalosti $n$ je pro dnešní počítače u čísel s tisíci ciframi prakticky nemožné. Právě v tom spočívá síla šifry.
```

Proces šifrování a podpisu

Úkon	Kdo co dělá	Výsledek
Šifrování	Odesílatel použije **veřejný klíč** příjemce.	Pouze příjemce může zprávu přečíst svým soukromým klíčem.
Digitální podpis	Odesílatel použije svůj **soukromý klíč**.	Kdokoliv může veřejným klíčem odesílatele ověřit, že podpis je pravý.

Praktické využití RSA

RSA se dnes málokdy používá k šifrování celých velkých souborů (protože je pomalé). Místo toho funguje jako „přepravka“:

- **SSL/TLS (HTTPS):** RSA se použije k bezpečnému předání krátkého symetrického klíče, kterým se pak šifruje zbytek komunikace (pomocí rychlé šifry AES).
- **SSH:** Pro bezpečné přihlašování k serverům bez hesla.
- **PGP / GPG:** Pro šifrování e-mailů.

Bezpečnost a délka klíče

S rostoucím výkonem počítačů musí růst i délka RSA klíčů, aby odolaly útokům hrubou silou:

- **1024 bitů:** Dnes považováno za nebezpečné a nedostatečné.
- **2048 bitů:** Současný standard pro běžné zabezpečení.
- **4096 bitů:** Vysoce bezpečné, používané tam, kde je vyžadována extrémní ochrana.

Budoucnost: S nástupem kvantových počítačů by mohlo být RSA prolomeno pomocí tzv. Shorova algoritmu. Proto se již dnes vyvíjí „post-kvantová kryptografie“.

Související pojmy: Asymetrické šifrování, SSL/TLS, AES, Prvočísla, Digitální podpis, SSH, PGP.