

Kryptografie: Základ bezpečných plateb

Kryptografie transformuje čitelná data (plain text) na nečitelný šifrovaný text (cipher text). V digitálních platbách se používají dvě hlavní rodiny šifer a jedna speciální funkce.

1. Symetrická kryptografie (Tajný klíč)

U symetrického šifrování se pro zašifrování i dešifrování používá **tentýž klíč**. Je to jako trezor, ke kterému mají obě strany identický klíč.

- **Hlavní algoritmus: AES** (Advanced Encryption Standard).
 - **Výhoda:** Extrémní rychlost. Ideální pro šifrování velkých objemů dat (např. databází s údaji o klientech).
 - **Nevýhoda:** Problém s bezpečným předáním klíče mezi stranami.
-

2. Asymetrická kryptografie (Veřejný a soukromý klíč)

Tento systém (PKI - Public Key Infrastructure) používá dvojici klíčů. Co jeden zamkne, druhý odemkne.

- **Veřejný klíč (Public Key):** Může ho znát kdokoli. Slouží k zašifrování zprávy pro mě.
 - **Soukromý klíč (Private Key):** Musí zůstat v tajnosti. Pouze já jím mohu dešifrovat zprávy určené mně.
 - **Využití:** Digitální podpisy a výměna klíčů.
 - **Algoritmy:** RSA, **ECC** (Elliptic Curve Cryptography - modernější, rychlejší, bezpečnější).
-

3. Hašovací funkce (Otisky dat)

Hash není šifra, protože se nedá „dešifrovat“. Je to jednosměrná funkce, která z libovolně velkých dat vytvoří unikátní řetězec fixní délky.

- **Využití:** Ukládání hesel (server neukládá heslo, ale jeho hash) a kontrola integrity (změna jediného bitu v objednávce zcela změní výsledný hash).
 - **Algoritmus: SHA-256** (používaný i v Bitcoinu).
-

4. TLS/SSL: Šifrování na cestě

Když platíte na webu, vaše prohlížeč a server vytvoří bezpečný kanál pomocí protokolu **TLS**

(Transport Layer Security).

1. ****Handshake:**** Server pošle prohlížeči svůj certifikát s veřejným klíčem.
2. ****Výměna:**** Prohlížeč ověří certifikát a pomocí asymetrické kryptografie si se serverem dohodnou dočasný "relační klíč".
3. ****Přenos:**** Samotná data (číslo karty) už tečou pomocí bleskové ****symetrické šifry**** (AES) s tímto relačním klíčem.

5. Tokenizace v platebních systémech

Specifická aplikace kryptografie v e-commerce, kterou vyžaduje [PCI DSS](#).

- Místo ukládání čísla karty (PAN) vygeneruje platební brána náhodný řetězec – **token**.
- Token je pro útočníka bezcenný, protože z něj nelze matematicky získat zpět číslo karty. Mapování probíhá v super-bezpečném trezoru poskytovatele (Vault).

Související články:

- [PCI DSS a bezpečnost dat](#)
- [Blockchain: Kryptografie v akci](#)
- [Zabezpečení webu \(HTTPS\)](#)

Tagy: it cryptography security encryption tls hashing fintech

From:
<https://www.serviceit.cz/> - IT ENCYKLOPEDIE

Permanent link:
https://www.serviceit.cz/doku.php?id=it:sw:cryptography_basics

Last update: **2026/01/02 20:09**

