



EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání



Kryptologie

*Moderní kryptologie:
Algoritmy asymetrické kryptografie*

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204

Obsah prezentace

- Algoritmus RSA
- Algoritmus DSA
- Srovnání systémů RSA, DSA a odvozených nástaveb ECC

1. Algoritmus RSA

Asymetrická kryptografie: RSA

- Vznik v roce 1977
- Pojmenován podle iniciálů autorů Rivest, Shamir, Adleman
- Šifra s veřejným klíčem, jedná se o první dostupný algoritmus, který je vhodný jak pro digitální podepisování, tak šifrování.
- Používá se i dnes, přičemž při dostatečné délce klíče je považován za bezpečný (2048 - 4096b) .

Asymetrická kryptografie: RSA

- Algoritmus je založen na předpokladu obtížnosti rozložit velké číslo na součin prvočísel – faktorizace.
- Z čísla $n = p * q$ je v rozumném čase prakticky nemožné zjistit činitele p a q .
- Naproti tomu násobení dvou velkých čísel je elementární úloha.
- **Fundamental theorem of arithmetic:**
 - Every integer greater than 1 either is a prime number itself or can be represented as the product of prime numbers [1].

Princip RSA - generování klíčů

- Síla této šifry tedy spočívá v tom, že dosud nebyla objevena metoda, jak rozložit velká čísla na prvočísla - faktorizace.
- V danou chvíli není ani zcela jisté zda je vůbec možné takovouto metodu objevit.
- Pokud se tak ovšem stane, bude tato šifra nepoužitelná.

RSA - útok

- S délkou klíče stoupá obtížnost prolomení šifry.
- Délka v současné době (256,512,1024,2048,3072,4096,8192)bitů.
- V současné době šifra považována za (prozatím) bezpečnou.
- Problémem může být případná úspěšná implementace kvantového počítače.

RSA - útok

- S rostoucím výpočetním výkonem, roste délka klíče, který je možno považovat za bezpečný.

=> Neustále klesá efektivita šifry!

- Proto začaly vznikat další asymetrické šifry, například kryptografie založená na eliptických křivkách.

Princip RSA - generování klíčů

- Zvolí se dvě různá velká náhodná prvočísla **p** a **q**
- Vypočítá se jejich součin **n = p * q**.
- Vypočte se hodnota Eulerovy funkce: **$\phi(n) = (p - 1)(q - 1)$** .

Příklad dle: [2]

Princip RSA - generování klíčů

- Zvolí celé číslo **e** menší než $\phi(n)$, které je s $\phi(n)$ nesoudělné.
- Nalezne se číslo **d** tak, aby platilo: $\mathbf{d * e \equiv 1 \pmod{\phi(n)}}$
- Jestli **e** je prvočíslo tak $\mathbf{d = (1+r*\phi(n)) / e}$, kde $\mathbf{r = [(e-1)\phi(n)^{(e-2)}]}$

Příklad dle: [2]

Princip RSA - generování klíčů

- Veřejným klíčem je dvojice (n, e) , přičemž n se označuje jako modul e se označuje jako šifrovací či veřejný exponent.
- Soukromým klíčem je dvojice (n, d) , kde d se označuje jako dešifrovací či soukromý exponent.
- Veřejný klíč se poté uveřejní.
- Soukromý klíč se naopak uchová v tajnosti.

Použití RSA

- Šifrování:
 - Šifrování je jednoduchá matematická operace $c = m^e \bmod n$
 - kde **m** - zpráva, **c** - šifra
- Dešifrování:
 - Dešifrování je opět jednoduchá matematická operace $m = c^d \bmod n$
 - kde **m** - zpráva, **c** - šifra

2. Algoritmus DSA

DSA - algoritmus digitálního podpisu

- DSA je založeno na problému výpočtu diskretního logaritmu.
- Využívá hash funkce a základní operace modulární aritmetiky (modulární inverze, umocňování, násobení a sčítání).
- Ověření podpisu je výpočetně náročnější než podepsání.
- DSA ověřování lze považovat za časově méně náročné nežli u RSA.
- Příklad algoritmizace a workflow: [3], [4].

3. Srovnání RSA, DSA a systémů s ECC

Srovnání RSA, DSA a EC variant

	RSA	DSA	ECC
Matematický problém	Faktorizace součinu prvočísel	Diskrétní logaritmus	Diskrétní logaritmus eliptických křivek
Řešení matematického problému	Číselné síťové pole (GNFS) [5]	Číselné síťové pole (GNFS) [5]	Pollardeho algoritmus pro diskrétní logaritmus [6]
Časová náročnost řešení matematického problému	subexponenciální	subexponenciální	exponenciální

Srovnání RSA, DSA a EC variant

Bezpečnost (bity)	Minimální délka klíče v bitech		
	RSA	DSA	ECC
80	1024	1024	160
112	2048	2048	224
128	3072	3072	256
192	7680	7680	384
256	15360	15360	512

Seznam odkazů

- [1] Fundamental Theorem of Arithmetics. [online]. Dostupné z: https://en.wikipedia.org/wiki/Fundamental_theorem_of_arithmetic
- [2] RSA. [online]. Dostupné z: <https://cs.wikipedia.org/wiki/RSA>
- [3] Digital Signature Algorithm. [online]. Dostupné z: https://en.wikipedia.org/wiki/Digital_Signature_Algorithm
- [4] ZEMAN, Václav, Zdeněk Martinásek. Kryptografie v Informatice. VUT v Brně, 2014.
- [5] Number Field Sieve. [online]. Dostupné z: <http://mathworld.wolfram.com/NumberFieldSieve.html>
- [6] Generic Algorithms for the Discrete Logarithm. [online]. Dostupné z: <https://math.mit.edu/classes/18.783/2017/LectureNotes10.pdf>



EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MŠMT
MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY

Děkuji za pozornost

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204



Doc. Ing. Roman Šenkeřík, Ph.D.
FAI, Ústav informatiky a umělé inteligence