Deterministický chaos v kryptografii

Adéla Kovářová

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Adéla Kovářová**
Osobní číslo:	**A19471**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Softwarové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Deterministický chaos v kryptografii**
Téma práce anglicky:	**Deterministic Chaos in Cryptography**

Zásady pro vypracování

1. Vysvětlete související terminologii.
2. Popište možnosti uplatnění deterministického chaosu v kryptografii.
3. Demonstrujte využití deterministického chaosu v kryptografii praktickou ukázkou.
4. Zvolte vhodný programovací jazyk.
5. Jednotlivé kroky aplikace deterministického chaosu zdokumentujte a okomentujte.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. CIMINO, Al. Příběh kryptologie: od starověkých šifer po kvantovou kryptografii. Přeložil Marek ČTRNÁCT. Praha: Dobrovský, 2018. Knihy Omega. ISBN 9788073908874.
2. BURDA, Karel. Úvod do kryptografie. Brno: Akademické nakladatelství CERM, 2015. ISBN 9788072049257.
3. OULEHLA, Milan a Roman JAŠEK. Moderní kryptografie. [Praha]: IFP Publishing, 2017. ISBN 9788087383674.
4. BUDIŠ, Petr. Elektronický podpis a jeho aplikace v praxi. Olomouc: ANAG, 2008. Právo (ANAG). ISBN 9788072634651.
5. KALABUS, Radek. Deterministický chaos a jeho využití v kryptografii. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 47 s. Dostupné také z: http://hdl.handle.net/10563/14199. Tomas Bata University in Zlín. Faculty of Applied Informatics, Ústav aplikované informatiky. Vedoucí práce Giesl, Jiří.
6. HORÁK, Jiří, Ladislav KRLÍN a Aleš RAIDL. Deterministický chaos a podivná kinetika. Praha: Academia, 2007. ISBN 9788020015310.
7. HORÁK, Jiří, Ladislav KRLÍN a Aleš RAIDL. Deterministický chaos a jeho fyzikální aplikace. Praha: Academia, 2003. ISBN 9788020009104.

Vedoucí bakalářské práce: **Ing. Lukáš Králík, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **2. prosince 2022**
Termín odevzdání bakalářské práce: **26. května 2023**

L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 7. prosince 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne

Adéla Kovářová, v.r.
podpis studenta

ABSTRAKT

Tato bakalářská práce se zabývá deterministickým chaosem v kryptografii a jeho aplikaci při šifrování. V teoretické části jsou vysvětleny základní pojmy kryptografie, deterministický chaos a matematické rovnice využívané pro generování deterministického chaosu. Praktická část obsahuje postup implementace programu pro šifrování s využitím logistické mapy.

Klíčová slova: deterministický chaos, kryptografie

ABSTRACT

This bachelor's thesis deals with deterministic chaos in cryptography and its application in encryption. In the theoretical part, the basic concepts of cryptography, deterministic chaos and mathematical equations used to generate deterministic chaos are explained. The practical part contains the implementation procedure of the encryption program using the logistic map.

Keywords: deterministic chaos, cryptography

Děkuji vedoucímu této bakalářské práce Ing. Lukáši Králíkovi, Ph.D. za vedení práce.

V neposlední řadě bych chtěla poděkovat sobě. Chtěla bych sama sobě poděkovat za sebedůvěru. Děkuji za všechnu tu tvrdou práci, kterou jsem vynaložila. Chci si poděkovat za to, že jsem si nebrala žádné dny volna a děkuji, že jsem to nikdy nevzdala.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Na světě existuje plno způsobů, kterým lze zašifrovat zprávy a zajistit tak bezpečný přenos informace. Vědci zkoumají různé možnosti zabezpečení zpráv, a protože post kvantová doba může nastat kdykoliv, je toto téma aktuálnější než kdy dříve. Deterministický chaos přináší jednu z potencionálních možností zabezpečení informací v dalších letech. Deterministický chaos přináší nový pohled na kryptografii, kdy se využívá nestabilního a deterministického chování chaotických systémů. Chaotické systémy jsou charakterizovány svou citlivostí na počáteční podmínky, což znamená, že malé změny ve vstupních hodnotách mohou způsobit výrazné rozdíly ve výstupu. Tato vlastnost poskytuje možnost vytvářet efektivní kryptografické postupy. Tato práce se zaměřuje na analýzu a popis využití deterministického chaosu v kryptografii. Tato práce zkoumá chaotické matematické funkce, které slouží k ochraně citlivých informací. Dále implementujeme rovnici logistické mapy jako funkci pro vytváření šifrovaného textu.

I. TEORETICKÁ ČÁST

1 TERMINOLOGIE NUTNÁ PRO POROZUMĚNÍ TEXTU

Jelikož se práce zaobírá odbornými tématy, budou se zde vyskytovat odborné názvy. Je tedy vhodné ještě před zahájením četby pochopit klíčové pojmy, které se frekventovaně vyskytují v této práci.

1.1 Kryptografie

Pojem kryptografie vychází z řeckého slova kryptos, které se překládá jako "skrytý", lze tedy odvodit, že se jedná o vědu zkoumající skrývání informací. Přesněji pojmem kryptografie rozumíme matematický aparát využíván pro vytvoření šifer a jejich analýzu. Často se zaměňuje s podobným termínem – kryptologií, i když se na první pohled pojmy mohou zdát stejné, opak je pravdou. Kryptologie se také zabývá matematickými návrhy, ale k tomu ještě studuje kryptoanalýzu a steganografii. Kryptoanalýza analyzuje text v naději, že najde vodítko, kterým lze zprávu rozšifrovat. Steganografie se zase snaží ukrýt informaci poněkud nevšedně, zatímco kryptografie informaci zašifruje a otevřeně ji "vypustí do světa", steganografie samotnou zprávu ukrývá tak, aby se o ní vůbec nevědělo (např.: schováním do obrázků). [1]

1.1.1 Otevřený a šifrovaný text

Otevřený text je důležitým pojmem v kryptografii, protože slouží jako vstup pro šifrovací algoritmy. Otevřený text zpráva je posloupnost symbolů z nějaké abecedy. Kvalita kryptografického algoritmu závisí na jeho schopnosti šifrovat otevřený text tak, aby byl šifrovaný text bezpečný a aby nebylo možné jej snadno prolomit bez platného klíče. Šifrovaný text je transformovaný otevřený text do nečitelné podoby, aby byly informace chráněny před neoprávněným přístupem. Tím se zajišťuje, že pouze osoby s odpovídajícími dešifrovacími klíči nebo znalostmi budou schopny rozluštit obsah zprávy. Existuje mnoho různých metod šifrování, které se liší v závislosti na použitém algoritmu. [22]

1.1.2 Asymetrické a symetrické šifrování

Šifrovaná komunikace je možná s využitím asymetrických i symetrických šifer. Rozdíl spočívá v tom, že při asymetrickém šifrování jsou klíče přijímače a vysílače odlišné, tudíž klíč, kterým se zpráva zašifruje, může být zveřejněn, aniž by byl někdo schopen rozšifrovat zprávu. U symetrické šifry je klíč pro šifrování i rozšifrování stejný. Asymetrické šifrování také umožňuje další funkce, například digitální podpis. Při použití soukromého klíče pro

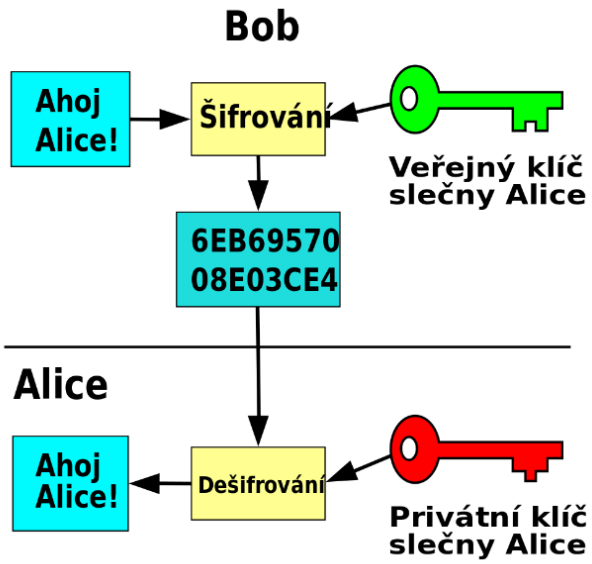
podpis zprávy je možné ověřit, že zpráva pochází od příslušného uživatele a nebyla pozměněna během přenosu. Matematické operace používané v asymetrických algoritmech jsou náročnější než v symetrických algoritmech, což vede k pomalejšímu procesu šifrování a dešifrování Dnes se používá kombinace obou, zpráva se symetricky zašifruje a klíč se zašifruje asymetricky. [2]

1.1.3 Klíče a princip fungování asymetrických klíčů

Kryptografie využívá klíče, které měl znát jen odesílající a příjemce. Klíče umožňují šifrovat nebo dešifrovat symboly abecedy. Klíče se mohou pro odesílajícího a příjemce lišit, v takovém případě mluvíme o asymetrickém šifrování, které je mnohem složitější, zároveň ale také bezpečnější. [9]

Princip fungování veřejného a soukromého klíče je založen na jednocestných operací. Příkladem těchto operací je například dodnes využívaná šifra RSA, která používá faktorizaci na prvočísla. Zašifrovat text je snadné, vyberou se dvě velmi velká čísla a vynásobí se. Ovšem pro rozšifrování je zapotřebí provést rozklad součinu na činitele, což by dnešní počítače dokázaly za několik set biliónů let. [10]

Asymetrická komunikace spočívá v tom, že nejdříve jsou vygenerovány páry klíčů. Veřejné klíče nejsou uschovány, naopak bývají volně dostupné pro kohokoliv, kdo chce danému uživateli poslat zašifrovanou zprávu. Aby se zabránilo i možnému nebezpečí při předávání soukromého klíče, odesílatel zprávu zašifruje veřejným klíčem a pošle ji příjemci, který zprávu zašifruje vlastním veřejným klíčem a pošle ji zpět. Odesílatel po zpětném obdržení zprávu rozšifruje pomocí jeho privátního klíče a opět pošle příjemci, ovšem zpráva zůstává pořád zašifrována příjemcem. Konečně příjemce rozšifruje zprávu jeho privátním klíčem a dozvídá se danou informaci. [9][20]



Obrázek 1 asymetrické šifrování

1.1.4 Proudové a blokové šifry

Primitivním rozdílem mezi symetrickými kryptosystémy je klasifikace na proudové a blokové šifry. Proudová šifra funguje tak, že symbol po symbolu vytváří sekvenci šifrových symbolů z abecedy. Bloková šifra pracuje s blokem symbolů a používá šifrovací algoritmus. Blokové šifry jsou silnější než proudové šifry a jsou častěji používány v moderní kryptografii. Příklad blokové šifry je například Playfairova substituční šifra, DES nebo AES. [9]

1.1.5 Entropie

Entropie je pojem, který v kontextu informační teorie a statistiky představuje míru nejistoty nebo nepředvídatelnosti v datech, zatímco informace je míra určitosti. Vyjadřuje, jak moc jsou data neuspořádaná nebo nepravidelná. Čím vyšší entropie, tím více informací nesou data a tím méně jsou předvídatelná. Pro binární systémy je měřena v bitech. Entropie se vypočítává pomocí pravděpodobností výskytu jednotlivých symbolů v daném textu. Entropie je maximální, pokud je výskyt všech symbolů stejně pravděpodobný a informace je nejvíce rozptýlena. Naopak, pokud některé symboly mají vyšší pravděpodobnost výskytu než ostatní, entropie je nižší a informace je více koncentrovaná. Pomáhá pochopit a měřit míru nejistoty a informačního obsahu v datech, což je klíčové pro efektivní manipulaci, analýzu a ochranu informací. [21]

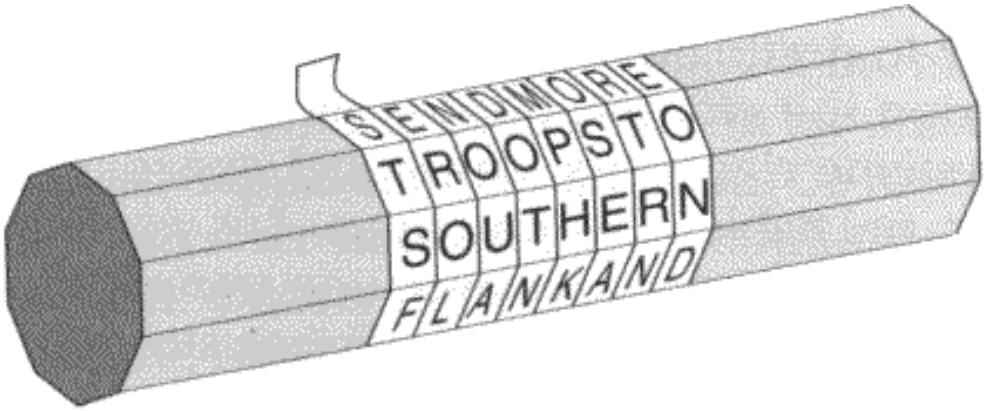
1.1.6 Frekvenční analýza

Frekvenční analýza je technika, která se používá v kryptografii k analýze dat, která může vést k odhalení informací v šifrovaném textu. Tato metoda se zaměřuje na analýzu četnosti výskytu jednotlivých znaků v textu. V různých jazycích existují určité vzorce četnosti znaků, které se opakují. Například v českém jazyce je hned za mezerou nejčastěji používaným znakem písmeno „e“ a nejméně často se vyskytuje písmeno „q“. Tuto pravidelnost lze využít při pokusu o prolomení šifry. Při frekvenční analýze se provádí zjišťování četností výskytu jednotlivých znaků ve šifrovaném textu. U znaků, které se v šifrovaném textu vyskytují nejčastěji můžeme předpokládat, že odpovídající často používaným znakům v původním textu. Frekvenční analýza nemusí vždy fungovat, zejména pokud je šifra navržena tak, aby zamaskovala četnosti znaků. V takových případech můžeme zkusit použít pokročilejší metody analýzy, jako je například analýza bigramů nebo trigramů. Frekvenční analýza je pouze jednou z mnoha technik v kryptografii a analýze dat, které se používají k prolomení šifer a analýze neznámých textů. [23][24]

1.1.7 Vývoj kryptografie

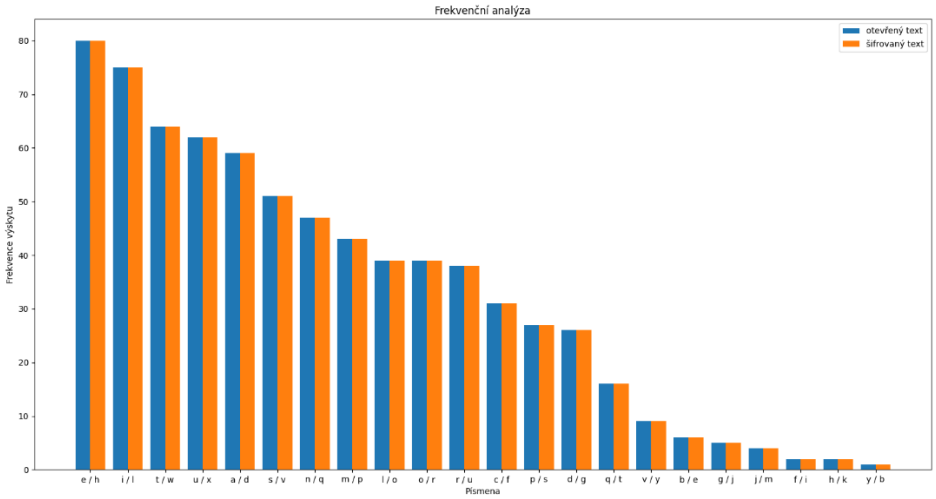
Někdy ve 20. století před naším letopočtem vznikly ve starověkém Egyptě první šifry, ovšem ne se záminkou skrýt zprávu, ale proto, aby se informace zdála důležitější, dnes jim říkáme hieroglyfy. Dokonce i v Biblických textech se vyskytují šifry, které ozvláštňují četbu. Například šifra Atbash byla používána k šifrování Hebrejské abecedy a vyskytuje se v knize Jeremjáš. Jedná se o jednoduchý převrácení abeceda, takže písmeno A by odpovídalo písmenu Z. [25][8]

Samozřejmě s vývojem jazyka se vyvíjela i potřeba zprávy utajit. Například při Sparťanských válkách bylo nutné, aby důležité informace nepadly do rukou nepřítele. Řekové tak využívali Skytalé, což je válec o předem domluveném průměru, na který se namotal papír a napsala se zpráva. Po odmotání sice zůstal jen papír s nesmyslným textem, ale rozšifrovat jej bylo jednoduché, stačilo jen papír namotávat na válce různých rozměrů, dokud nevznikl smysluplný text. [22]



Obrázek 2 Skytalé

Postupně se stávaly těžšími na rozluštění, proto časem vymizely. Další dochované šifry byly nalezeny v jiných vyspělých státech starověku. Jedna z nejznámějších historických šifer je Caesarova šifra. Tato šifra využívala substituci [1], samotný Caesar používal posun písmen o tři místa. [26]

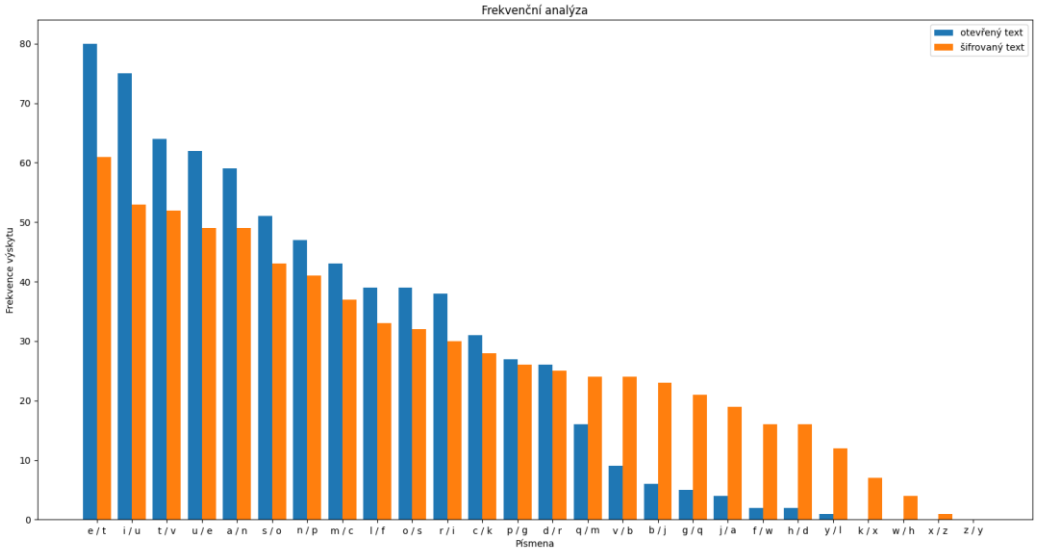


Obrázek 3 Frekvenční analýza Caesarovi šifry

Koncem 16. století se objevuje další revoluční metoda šifrování, která znemožnila jednoduše využít frekvenční analýzu pro dešifrování. Vigenèrova šifra využívá k šifrování heslo

[1] Substituce e typ šifrování, kde jsou znaky nebo jednotky textu nahrazeny jinými. [27]

libovolné délky a k dešifrování slouží čtverec o rozměrech 26x26, který obsahuje postupně posunuté abecedy. Pokud je heslo správně zvoleno, každé písmeno může být nahrazeno libovolným písmenem. I když byla tato šifra ve své době považována za nerozluštitelnou, ve skutečnosti to není pravda. [8]



Obrázek 4 Frekvenční analýza Vigenèrovi šifry

Dalším zlomovým okamžikem v historii šifrování je Enigma. Enigma je šifrovací stroj s komplexními elektrickým obvody, který Německo během 2. světové války požívalo pro utajení komunikace mezi spojenci. [8]

Rok 1976 byl pro kryptografii jedním z nejpříznivějších let. Na svět byl uveden nový kryptografický protokol s názvem Diffieho-Hellmanova výměna klíčů. Díky tomuto protokolu mohly být klíče veřejné. Položili tak základ asymetrické kryptografii. [10]

Šifra RSA vznikla krátce poté, když spojili své síly Ron Rivest, Adi Shamir and Leonard Adleman a navrhli šifru, která se stala jednou z nejpoužívanější na světě. Šifra je založená na prvočíselném počítání zbytkových tříd po dělení. Šifra se považuje za neprolomitelnou z důvodu neexistence kvantových počítačů, které by dokázaly faktorizovat velká čísla na součin prvočísel v dostatečném čase. [10]

AES je symetrická bloková šifra, která byla vynalezena v roce 1997 a v současné době je de facto standardem. AES na rozdíl od ostatních šifer pracuje s dvourozměrnými bloky.

Matice o rozměru 4x4, která se nazývá stavová matice používá čtyři transformace. Substituce bajtů, rotace řádků, substituce sloupců a přičtení iteračního klíče jsou operace využívány stavovou maticí pro zašifrování zprávy. [9]

1.2 Deterministický chaos

V encyklopedii Britannica slovo chaos je odvozeno od řeckého slova "χαοσ" a znamenalo nekonečný prázdný prostor, který existoval před všemi věcmi. V moderním jazyce je chaos označení pro stav nepořádku a nepravidelnosti, tak ho používá i teorie chaosu. [3]

Deterministický chaos je chaos, jehož časová závislost je deterministická. Jinými slovy existuje diferenciální nebo diferenční rovnice, která je dána počátečními podmínkami, na základě, kterých je možné určit budoucí chování systému. Diferenciální rovnice a diferenční rovnice jsou používány ke studiu změn v proměnných v čase. Diferenciální rovnice jsou matematické rovnice, které popisují změny proměnných, které jsou založeny na derivacích proměnných, které se mohou měnit. Pro vyřešení diferenciálních rovnic musíme určit všechna její řešení. Diferenční rovnice jsou matematické rovnice, které popisují změny proměnných v jednotlivých časových bodech. Výsledkem je nalezení vztahu pro n-tý člen posloupnosti diskrétních časových okamžiků nějaké veličiny. [4][19]

Deterministický pohyb se může dle předchozího textu zdát jako pravý opak chaosu, ale již v 19. století bylo objevena Hamiltonova rovnice, která je prvním úkazem chaotického deterministického pohybu. Trvalo poté několik desítek let, než bylo zjištěno, že i jednoduchá sada tří sdružených nelineárních diferenciálních rovnic prvního řádu může vést ke zcela odlišným trajektoriím. [2]

Fyzika je schopna vyřešit i velmi složité jevy a to tak, že je rozloží na jednodušší části, které umí řešit a ty pak opět složí zpět. Podmínkou je však to, že se systém chová lineárně, což znamená, že celek můžeme chápat jako součet částí. Další výhodou lineárního systému je, že částem systému můžeme porozumět, aniž bychom museli pochopit systém jako celek. U řady problémů je však jasné, že zákon, kterým se systém řídí je nelineární [2]. Analytické řešení takových rovnic nebylo možné. Přistupovalo se tedy k těmto problémům linearizací,

[2] Nelineární systém je takový systém, který obsahuje členy vyšších řádů, tudíž nelze použít rozklad na části a opětovné složení.

při níž se členy vyšších řádů zanedbaly. To přinášelo omezení platnosti na určitou oblast parametrů nebo určitou dobu trvání. Odchylky od výpočtů byly odsuzovány jako šum, poruchy apod., protože to bylo nepředpověditelné. [16]

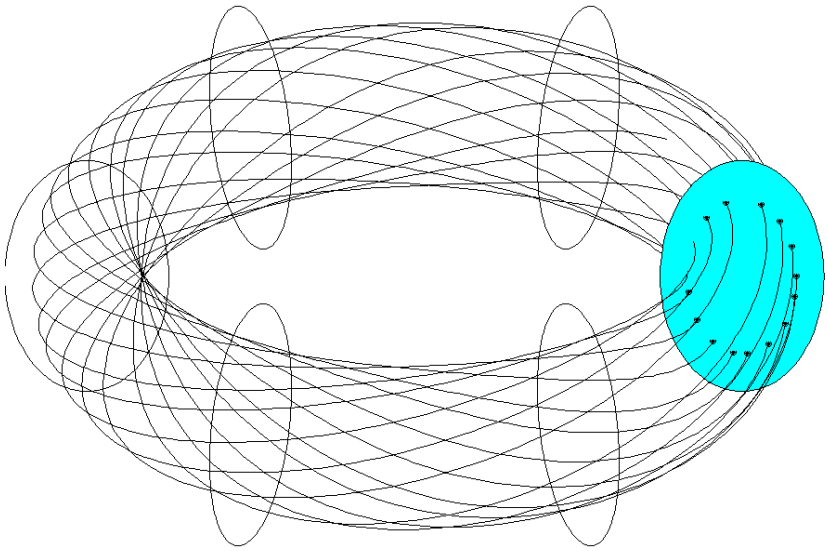
1.2.1 Historie teorie chaosu

V 17. století Isaac Newton jako první zdokumentoval oběžné dráhy planet a vysvětlil infinitezimální počet [3]. Díky jemu a mnoha dalším myslitelům již v 17. století bylo možno vybrat z podmínek určujících jev ty nejdůležitější a abstrahovat ode všech ostatních. Tím se podařilo najít prosté zákony vyjadřující nejdůležitější závislosti. [16]

Dalším významným objevem bylo v 19. století poincarého mapa. Poincaré se nechal inspirovat floquetovou myšlenkou, kde vyřadil prostřední aspekty trajektorie v periodickém lineárním systému. Poincare se intenzivně zabýval studiem složitých, nelineárních vysoko dimenzionálních systémů. Při svém výzkumu si všiml, že řešení těchto systémů nevykazují pravidelný charakter, ale opakují se a stále se vrací zpět do oblastí, kde vznikly. Poincaré se proto rozhodl definovat průřez toku níže dimenzionálního subprostoru a sledovat průsečík trajektorií procházející tímto subprostorem. Výsledkem tohoto sledování je soubor diskrétních hodnot iterací, které představují průsečík těchto trajektorií s podprostorem, podle kterého můžeme sestavit diferenční rovnice, které na rozdíl od diferenciálních, umíme řešit. Tento teoretický proces je nyní označován jako „Poincarého mapování“. Využití tohoto mapování spočívá v tom, že přesně zobecňuje průsečíky trajektorií s podprostorem a umožňuje iteraci za sebou. Poincaré došel k závěru, že uzavřené křivky ve fázovém prostoru odpovídají periodickým, příp. kvaziperiodickým dějům [4], zatímco neuzavřené nepravidelné křivky chaotickým pohybům. Poincaré, který je považován za přímého předchůdce oboru deterministického chaosu také formuloval, že v reálných systémech musí být entropie vždy větší než nula, což znamená že, v systému musí nastat alespoň nepatrná změna. [15][16]

[3] Infinitezimální počet, také známy jako kalkulus je matematický obor zabývající se hlavně diferenciálním a integrálním počtem.

[4] Kvaziperiodický děj je děj takový, jehož amplituda klesá s časem



Obrázek 5 Poincarého řez torusu

Deterministický chaos začal být uznávaným vědním oborem až v pozdní polovině 20. století, a to hlavně díky počítačům, které usnadnily matematické výpočty, takže i složité operace byly vyřešitelné v relativně krátkém čase. V roce 1972 Edward Norton Lorenz zveřejnil jeho výzkum zabývající se předvídatelností v meteorologii s názvem „Does the flap of a butterfly wing set off a tornado in texas?“. Lorenz začal nad touhle problematikou přemýšlet víc, když chtěl nasimulovat zemskou atmosféru. Do počítače zadal počáteční podmínky ve tvaru 12 desetinných čísel, které v každé iteraci byli přepočítány a vytištěny pro pozorování změn. Zlomový okamžik byl tehdy, když Lorenz zadal znovu jednu z iterací a pozoroval průběh. Pár počátečních iterací bylo stejných, ovšem v poslední iteraci byly výsledky z minulého kola drasticky odlišné od nových. Je tomu tak právě z toho důvodu, že Lorenz v druhém kole zadal danou iteraci jen se třemi desetinnými místy, zatímco počítač kalkuloval iteraci s šesti desetinnými čísly. Citlivá závislost na počáteční podmínky je jeden z charakteristických znaků deterministického chaosu. Kvůli této citlivosti nejsme dodnes schopni s předpovědět, jaké počasí bude za týden. [17][18][4]

1.2.2 Hamiltonova rovnice a jak souvisí s chaosem

Již v 19. století bylo objeveno, že určité mechanické systémy, jejichž časový vývoj je řízený Hamiltonovou rovnicí, jsou schopny vytvářet chaotický pohyb. Rovnice je dána třemi veličinami, a to souřadnicemi a momentem hybnosti (narozdíl od Lagrangiánu, kde pracujeme s rychlostí) a případně časem. Obecně je tedy hamiltonián (1).

$$H = H(qj, pj, t) \tag{1}$$

Jako příklad tohoto systému si můžeme vzít harmonický oscilátor. Poloha kmitajícího tělesa, jež je připevněno k pružině je dána x(t), hybnost tělesa je dána p(t) a pružnost a hmotnost jsou označovány k a m. Kinetickou energii lze vypočítat pomocí vzorce (2) a potenciální energii pomocí vzorce (3).

$$E_k = \frac{1}{2}mv^2 \tag{2}$$

$$E_p = \frac{1}{2}kx^2 \tag{3}$$

Rozdílem kinetické a potenciální energie získáme Lagrangeova funkci, která je pohybovou rovnicí oscilátoru. Pro získání Hamiltonovy funkce musíme použít Legendrovu transformaci na získnou Lagrangeovu funkci. Hamiltonova rovnice pracuje s momentem hybnosti a díky tomu je možné získat body fázového prostoru, což umožní systematicky sledovat chaotické systémy. Hamiltonova funkce pro oscilátor (4) je jednou z nejjednodušších rovnic, která vytváří chaos. [5]

$$H = \frac{1}{2}mp^2 + \frac{1}{2}kx^2 \tag{4}$$

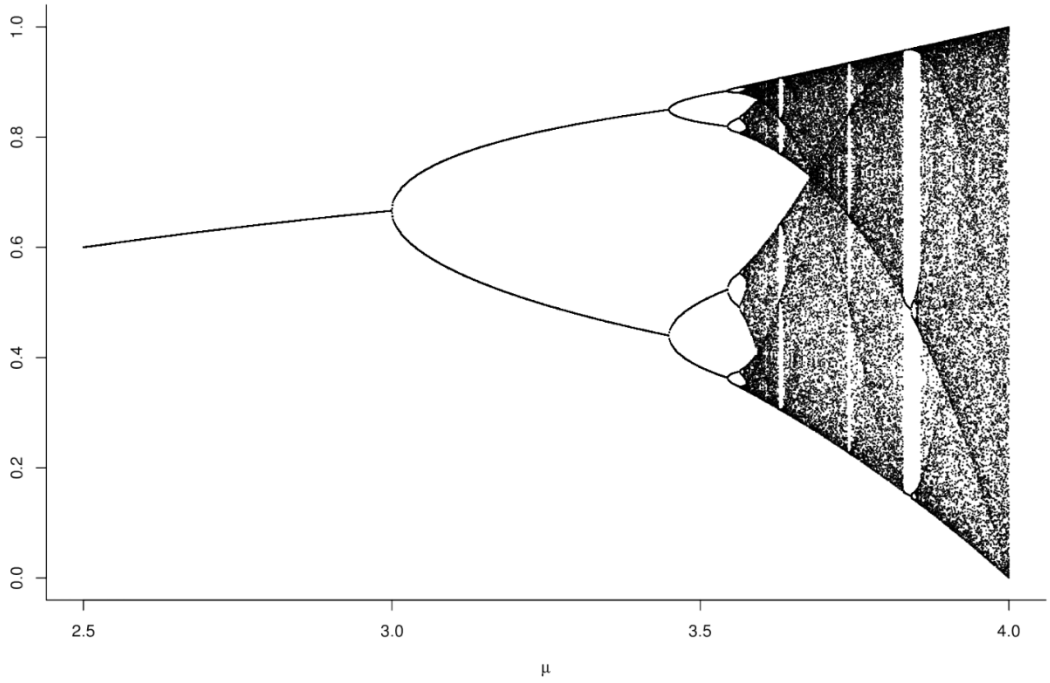
1.2.3 Logistická mapa

Další zajímavá rovnice, která představuje skvělé vlastnosti chaosu je logistická mapa. Je to jednoduchá rovnice, která se vyskytuje i v přírodě, například u vývoje populace.

$$x_{n+1} = rx_n(1 - x_n) \tag{5}$$

Pokud bychom si pro lepší vizualizaci chtěli rovnici představit na vývoji populace, tak by „x“ bylo procentuálním maximem populace (0–1) a “r“ by byla rychlost vývoje. Například pokud by bylo r =2 populace se bude zvětšovat 2x každý rok. Jako v přírodě, tak ani v reálném světě se populace nemůže zvětšovat do nekonečna, proto je nutno přidat (1 - xn). „n“ si můžeme představit jako počet let, kterým vývoj prošel. Graficky je znázorněním téhle

rovnice jen převrácená parabola. Pokud zvolíme náhodné procentuální maximum populace „x“ a náhodné zvětšování populace, dojdeme nakonec k ustálení a stabilizaci populace, tento stav nazýváme ekvilibrium. Pokud bychom změnili x (počáteční populaci), prvních pár let by byly vidět znatelné rozdíly, ale po pár iteracích by opět došlo ke stejnému výsledku, a to ekvilibriu. Naopak pokud by bylo změněno „r“, ekvilibrium populace by se buď snížilo nebo zvýšilo.



Obrázek 6 Graf logistické mapy

2 VYUŽITÍ DETERMINISTICKÉHO CHAOSU V KRYPTOGRAFII

Chaotický pohyb znamená, že signál vykazuje nepravidelné a aperiodické chování v čase. Výhoda použití chaotických systémů v kryptografii spočívá v tom, že jsou velmi odolné vůči útokům hrubou silou a mají velkou kapacitu pro ukládání dat. Navíc jsou chaotické systémy často rychlé a mají nízké náklady na implementaci. Existují různé způsoby, jak použít deterministický chaos v kryptografii. Jedním z nich je použití mapující funkce, která transformuje vstupní data na náhodnou posloupnost. Další možností je použití chaotických oscilátorů, které generují signály s vysokou entropií a používají se jako zdroj náhodných čísel. Deterministický chaos v kryptografii využívá obtížnosti předpovědět budoucí chování systému. Totéž platí, když se díváme do minulosti chaotických systémů a pokoušíme se identifikovat počáteční příčiny. Je však třeba mít na paměti, že použití deterministického chaosu v kryptografii není bez rizika a některé kryptografické systémy, které využívají chaotické systémy, byly analyzovány a jejich bezpečnost byla zpochybněna. Proto je důležité pečlivě zvažovat spolehlivost takových systémů před jejich implementací. [6]

2.1 Spojitost mezi kryptografií a chaosem

Chaotické systémy jsou implementovány s deterministickými nelineárními dynamickými systémy, které jsou schopny produkovat deterministickou pseudonáhodnost vyžadovanou v kryptografii. Existují také určité nevýhody při používání chaosu v kryptografii. Jedním z hlavních problémů je, že chaotické systémy jsou deterministické, což znamená, že při znalosti počátečních podmínek mohou být předpovězeny budoucí stavy systému. To může vést k porušení bezpečnosti kryptografického systému. Proto musí být pečlivě zvažováno, jaké chaotické systémy jsou vhodné pro použití v kryptografii a jaké bezpečnostní mechanismy by měly být použity k minimalizaci rizika prolomení kryptografického klíče. Celkově lze říci, že spojení mezi kryptografií a chaosem spočívá v tom, že oba obory se snaží chránit data před útoky a využívají matematické funkce k dosažení tohoto cíle. Chaotické systémy mohou poskytovat vhodný zdroj náhodných čísel a šifrovacích klíčů pro kryptografické systémy, a proto jsou v tomto oboru stále více zkoumány a používány. [7]

Tabulka 1 Alvarez & Li, 2006

Chaotická charakteristika Kryptografická vlastnost	Kryptografické vlastnosti	Popis
Ergodicita Vlastnost míchání Automatická podobnost	Zmatek	Výstup systému se zdá podobný pro jakýkoli vstup
Citlivost na počáteční podmínky a regulační parametry	Difuze	Malý rozdíl ve vstupu vytváří velmi odlišný výstup
Determinističnost	Deterministická pseudonáhodnost	Deterministický postup, který vytváří pseudonáhodnost
Komplexita	Algoritmická složitost	Jednoduchý algoritmus, který produkuje vysoce komplexní výstupy

Tato tabulka shrnuje souvislost mezi chaosem a kryptografií. Díky těmto souvislostem mohli vědci a výzkumníci ve 20. a 21. století přijít na některé kryptosystémy.

2.2 Známé možnosti využití deterministického chaosu

Deterministický chaos je využíván jak v analogových, tak i digitálních systémech. Analogové systémy využívají jako chaos jako zdroj pro generování náhodných chaotických čísel a klíčů. Jako generátor chaotických signálů může být využito velké množství věcí, například elektromagnetický šum nebo například Rösslerův nebo Lorenzův oscilátor, což jsou elektronické obvody, které generují chaos. Chaos také může být využit pro modulaci signálu, kde se využívá jeho citlivost na počáteční podmínky, což ztěžuje jeho rozpoznání neautorizovanými příjemci. Digitální kryptografické systémy využívají chaotické funkce pro generování klíčů pro šifrování a dešifrování dat.

2.2.1 Aditivní maskování chaosu

Aditivní maskování chaosu je technika kryptografie, která využívá chaotické funkce k maskování šifrovacích klíčů a zabezpečení přenosu dat. Tento postup funguje tak, že se k původnímu datovému proudu přičte náhodný šumový signál generovaný chaotickou funkcí. Tento šumový signál je znám pouze odesílateli a příjemci, a proto umožňuje oběma stranám přístup k původním datům, zatímco potenciálním útočníkům brání v přístupu k těmto datům. Aditivní maskování chaosu může být použito v různých kryptografických aplikacích, včetně bezpečného přenosu dat mezi dvěma stranami. Například, pokud dvě strany chtějí komunikovat přes veřejnou síť, mohou použít aditivní maskování chaosu k šifrování datového proudu, takže pouze příjemce bude schopen dešifrovat původní data pomocí znalosti maskovací funkce. Dalším využitím aditivního maskování chaosu je v ochraně citlivých informací při výpočtech v decentralizovaných systémech. Například v blockchainu se často používá tato technika ke zabezpečení transakcí a údajů, aby byly chráněny před neautorizovaným přístupem a útoky. Celkově lze říci, že aditivní maskování chaosu poskytuje další vrstvu zabezpečení pro kryptografické systémy a může být využíváno v různých aplikacích pro ochranu dat a informací.

2.2.2 Chaotické posouvání

Anglicky Chaotic shift keying je technika, která využívá chaotického signálu pro šifrování datových přenosů. Principem této techniky je posunování (shift) signálu podle klíče, který vychází z chaotické funkce. Při použití chaotického posouvání se nejprve vytvoří chaotický signál pomocí matematického modelu, který je náhodný. Tento signál se následně použije jako klíč pro šifrování datového proudu. Posouvání probíhá tak, že se data posunují o určitý počet bitů podle hodnoty chaotického signálu. Tato technika umožňuje šifrovat data takovým způsobem, že je obtížné odhalit původní data bez správného klíče. Chaotický signál totiž zajišťuje náhodnost a nemožnost jeho předpovědi, což znemožňuje útoky na šifrovaná data. Chaotické posouvání má využití všude, kde je potřeba bezpečně a spolehlivě přenášet data.

2.2.3 Chaotická modulace

Chaotická modulace je technika modulace, která využívá chaotických oscilátorů pro generování signálu k modulaci nosné vlny. Chaotické oscilátory jsou nestabilní a neperiodické, což znamená, že jejich signály jsou náhodné a zdánlivě nesouvisející. Tyto oscilátory se používají k vytvoření signálu, který je použit jako modulační signál pro nosnou vlnu. Výhodou chaotické modulace je to, že signál generovaný chaotickým oscilátorem může být velmi náhodný, a tedy těžko předvídatelný, což ztěžuje jeho odposlech a rušení. Tuto vlastnost využívají například moderní systémy pro zabezpečenou komunikaci. Nicméně, chaotická modulace je relativně složitá technika a vyžaduje sofistikované matematické algoritmy pro výpočet a řízení chaotických oscilátorů. Je také náchylná k rušení a náročná na nastavení, což může ovlivnit stabilitu a spolehlivost signálu.

2.2.4 Chaotické ovládání

Chaotické ovládání (anglicky "chaos control") je technika, která se používá pro řízení chaotických systémů, tedy systémů, kde jsou signály náhodné a neperiodické. Cílem chaotického ovládání je upravit chování takového systému, aby se choval předvídatelněji a stabilněji. Jednou z metod chaotického ovládání je tzv. stabilizace periodické dráhy. Tato metoda spočívá v tom, že se systém ovládá tak, aby se udržel na určité periodické dráze, která je známá a předvídatelná. Toho lze dosáhnout například pomocí tzv. P-stabilizace, kdy se do systému vkládá signál, kterým se ovládá jeho chování a udržuje ho na periodické dráze. Další metodou chaotického ovládání je tzv. synchronizace, kdy se dva nebo více chaotických systémů synchronizují na stejnou periodickou dráhu. Tato technika se často používá například v bezdrátové komunikaci, kdy se synchronizují vysílač a přijímač, aby mohly spolehlivě komunikovat. Kromě těchto metod existuje celá řada dalších technik chaotického ovládání, jako je například adaptivní ovládání, ovládání pomocí impulsů nebo ovládání pomocí náhodných signálů. Chaotické ovládání velmi užitečnou technikou, která umožňuje stabilizaci a řízení chaotických systémů i v mnoha dalších oblastech, jako jsou například fyzika, biologie, elektrotechnika a další.

2.2.5 S-Boxy

S-Box je základní stavební prvek některých blokových šifer, jako například v šifře AES. S-Box přijímá vstupní bity a generuje výstupní bity do předem dané substituční tabulky. S-Boxy slouží k nahrazování (substituci) jednoho bloku bitů za jiný blok bitů. Tento proces se

používá k narušení statistického charakteru dat a znesnadnění kryptoanalýzy. Šifry, které používají S-Boxy obvykle využívají několika vrstev těchto bloků pro zvýšení jejich bezpečnosti. Všechny tyto S-Boxy jsou navzájem nezávislé a při dešifrování musí být použita inverzní substituční tabulka pro každý S-Box. Výběr vhodné substituční tabulky pro S-Boxy je kritický pro zajištění bezpečnosti šifry. Musí být dostatečně složitý a náhodný, aby byl odolný vůči různým druhům kryptoanalýzy, jako je diferenciální kryptoanalýza nebo lineární kryptoanalýza. Výběr této tabulky může být výzvou, a proto se v kryptografii často používají algoritmy pro generování náhodných čísel a tabulek. Celkově lze říci, že S-Boxy jsou důležitým nástrojem pro zajištění bezpečnosti kryptografických šifer. S-boxy jsou hojně využívány i například v DES šifrování.

2.2.6 Searching based chaotické šifry

Searching based chaotické šifry jsou šifrovací algoritmy, které využívají chaotických oscilátorů pro generování klíče a následnou šifrování zprávy. Tyto algoritmy jsou založeny na principu hledání optimálního řešení v prostoru klíčů pomocí vyhledávacího algoritmu. Chaotické oscilátory jsou využity pro generování náhodných čísel, které jsou použity jako klíč pro šifrování zprávy. Tyto oscilátory jsou nestabilní a neperiodické, což zajišťuje velkou entropii v klíči a tedy vysokou bezpečnost šifrování. Pro vyhledávání optimálního řešení v prostoru klíčů se používají různé metody, jako například simulované ochlazování, genetické algoritmy nebo algoritmy optimalizace rojem částic. Tyto algoritmy hledají optimální klíč pro šifrování zprávy tak, aby byla zpráva co nejbezpečnější. Tyto šifry jsou velmi bezpečné šifrovací algoritmy, protože generovaný klíč je velmi náhodný a těžko předvídatelný. Tyto algoritmy jsou také velmi rychlé a efektivní, což umožňuje rychlé šifrování velkých objemů dat.

2.2.7 Celulární automat

Celulární automat je matematický model, který se skládá z mřížky buněk, kde každá buňka má určitý stav. Stav každé buňky se mění v závislosti na stavech jejích sousedních buněk a na pravidlech, která jsou aplikována na tuto mřížku. V kryptografii se Celulární automat využívá jako algoritmus pro šifrování dat. Šifrování pomocí Celulárního automatu se nazývá celulární šifrování a pracuje tak, že vstupní data jsou rozdělena do bloků a každý blok je zakódován. Výstup z Celulárního automatu pak slouží jako šifrovaná zpráva. V celulárním šifrování je důležitý počáteční stav buněk, který se volí náhodně a slouží k zajištění, aby byla

šifrovaná zpráva náhodná. Pravidly jsou matematické operace, které se aplikují na mřížku buněk. Tyto operace jsou aplikovány na základě stavů buněk a vytvářejí nový stav buněk. Klíčový prostor je prostor možných počátečních stavů buněk. Použití různých klíčů umožňuje generovat různé náhodné počáteční stavy a tím i různé šifry. Celulární šifrování je výhodné zejména proto, že umožňuje šifrování dat bez nutnosti vytvářet komplikované matematické operace, jako jsou v případě symetrických šifer, jako například AES. Tím se snižuje výpočetní náročnost algoritmu a zároveň zvyšuje jeho rychlost. Nicméně, stejně jako u jakékoliv jiné šifry, závisí bezpečnost celulárního šifrování na kvalitě klíče. Pokud je klíč nízké kvality nebo příliš krátký, může být šifra snadno prolomena pomocí brute-force útoku nebo jiných metod kryptoanalýzy. Celulární automat tedy představuje zajímavou alternativu ke klasickým kryptografickým metodám, která může být použita pro šifrování dat v situacích, kdy jsou nutné vysoké rychlosti a nízká výpočetní náročnost.

II. PRAKTICKÁ ČÁST

3 VÝBĚR VHODNÉHO PROGRAMOVACÍHO JAZYKA

Pro implementaci programu na šifrování s využitím deterministického chaosu je vhodné zvolit programovací jazyk, který umožňuje efektivní práci s matematickými funkcemi a výpočty. Některé programovací jazyky jsou přímo navrženy pro matematické výpočty a mohou být vhodné pro implementaci šifrovacího algoritmu s využitím deterministického chaosu.

Při volbě vhodného jazyka pro algoritmus jsem brala v úvahu především rychlost výpočtů a dostupnost knihoven pro matematické výpočty. Vybrala jsem Python, který je velmi populární programovací jazyk, který má mnoho knihoven pro matematické výpočty. Budu využívat například knihovnu NumPy, která umožňuje snadnou práci s maticemi, vektorovými výpočty a Fourierovou analýzou, což je užitečné pro implementaci šifrovacího algoritmu s využitím deterministického chaosu.

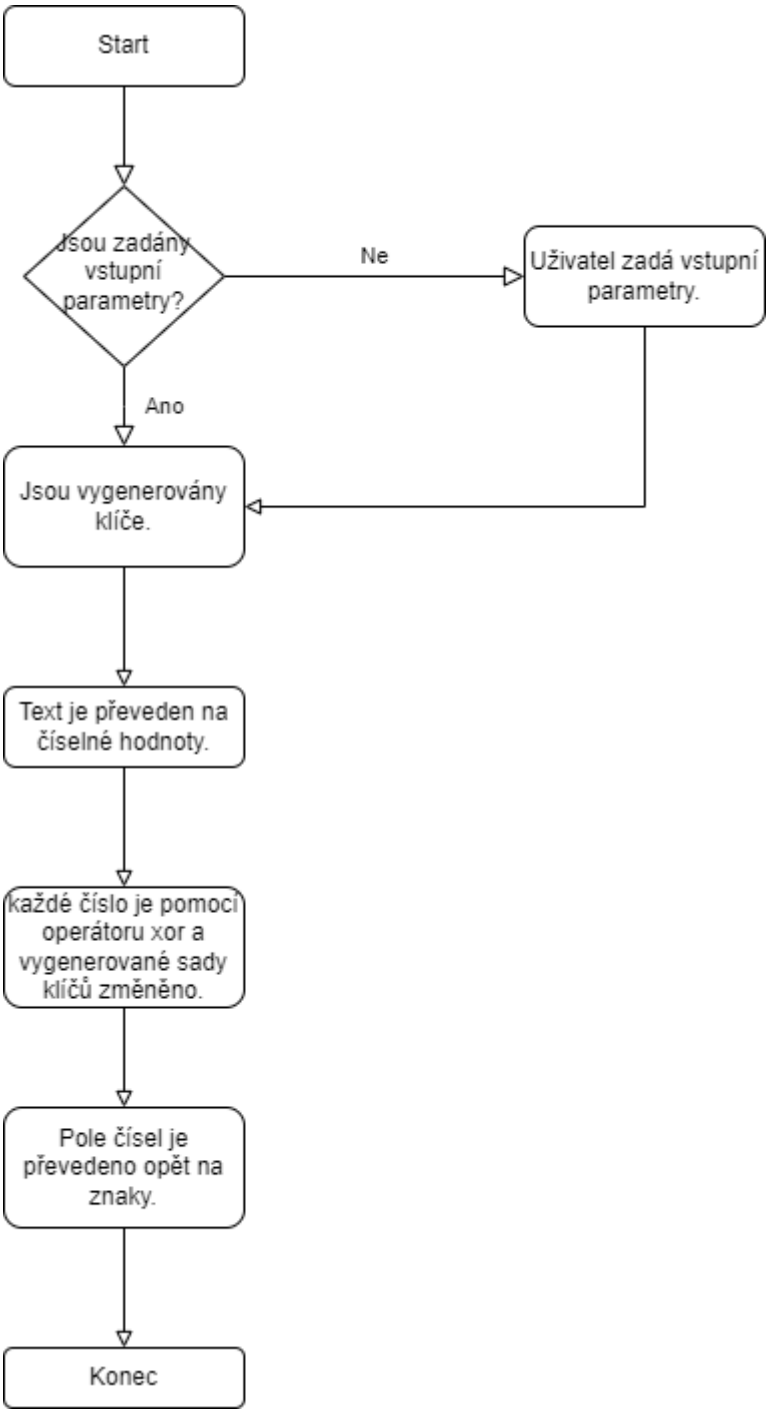
Další alternativou byl MATLAB a C/C++. MATLAB je programovací jazyk, který je přímo navržen pro matematické a numerické výpočty. Obsahuje mnoho vestavěných funkcí pro práci s maticemi, lineární algebrou a statistikou. C/C++ jsou nízkoúrovňové programovací jazyky, které umožňují efektivní práci s pamětí a výpočty. Pokud by pro mě bylo důležité dosáhnout vysoké rychlosti výpočtů, volila bych C.

3.1 Zvolení vhodné matematické funkce

Jako vhodnou funkci ukázky digitálního kryptografického systému jsem zvolila jednoduchou logistickou mapu, kterou jsme si představili v dřívějších kapitolách. Logistická mapa mi přišla jako nejlepší volba, jeden z hlavních důvodů je to, že uživatel dokáže jednoduše pochopit funkci jen ze samotného kódu, a tak lépe porozumět deterministickému chaosu a jak jej můžeme využít v kryptografii. Toto šifrování založené na logistické mapě není vhodné pro skutečné zabezpečené kryptografické aplikace. Tento příklad slouží spíše jako ukázka konceptu než jako doporučení pro použití v reálném světě.

3.2 Vývojový diagram pro šifrování pomocí logistické mapy

Ještě před samotnou implementací jsem si pro lepší orientaci vytvořila vývojový diagram. Na vytvoření diagramu jsem použila službu app.diagrams.net.



Obrázek 7 Vývojový diagram

3.3 Popis implementace šifrování pomocí logistické mapy

Prvním krokem při vývoji programu je pochopení, z čeho se bude vycházet. V kapitole 1.2.5 je vysvětlena logistická mapa. Což jen pro připomenutí je matematický model, který vykazuje chaotické chování a je definován rekurzivní rovnicí (5), kde „xn“ je aktuální hodnota a „r“ je parametr, který určuje chování mapy. Tahle znalost je nezbytná při implementování šifrovacího algoritmu.

Na začátku jsem zvolila hodnotu parametru „r“ a počáteční hodnotu „x“, aby se mi lépe začínalo s implementací, zvolila jsem hodnotu pro r = 4 a x = 0,4. Tyto parametry může uživatel dynamicky měnit, aby mohl pozorovat chaotické chování a vizuálně tak lépe porozumět chaosu. Pro vygenerování klíčů se musí sekvence chaotických kroků několikrát opakovat, tento parametr společně s parametry „r“ a „x“ jsem vložila do funkce „vygeneruj_klic“.

```
def vygeneruj_klic(r, X, iterace):
    klic = []
    for i in range(iterace):
        X = r * X * (1 - X)
        klic.append(int(X >= 0.5))
    return klic
```

Tato funkce se stará o vygenerování chaotických klíčů s použitím logistické mapy a to tak, že funkce logistické mapy je několikrát opakována a pokaždé vygeneruje desetinné číslo mezi 1 a 0. Tohle číslo je poté převedeno funkcí int() na celé číslo. Tak získám sekvenci 1 a 0, což používám jako klíč k šifrovacímu algoritmu.

Zde jsou hodnoty „x“ před převedením na celá čísla se zvolenými parametry „x“ a „r“:

0.96

0.15360000000000013

0.5200281600000003

0.9983954912280576

0.006407737294172653

0.02546671278776609

0.09927263731020608

0.3576703231667294

0.918969052370147

0.297859732624244

Dalším krokem je samotná implementace šifrovacího algoritmu. Funkce s názvem „sifruj“ převezme pole klíčů z uvedené funkce „vygeneruj_klic“ jako parametr „klic“ a parametr otevreny_text je text k zašifrování. Jako výsledek funkce je zašifrovaný text, který se vytvoří pomocí logického operátoru XOR, který nastaví bit na 1, pokud je pouze jeden ze dvou bitů 1. Porovnávám bity otevřeného textu s bitem klíče vygenerovaný algoritmem s použitím logistické mapy. Ke správnému fungování pomáhá také operátor modulo, který dohlíží na to, aby nedošlo k chybě z důvodu nedostatku vygenerovaných bitů v klíči.

```
def sifruj(otevreny_text, klic):
    sifrovany_text = []
    delka = len(otevreny_text)
    for i in range(delka):
        sifrovany_text.append(otevreny_text[i] ^ klic[i % len(klic)])
    return sifrovany_text
```

Aby šifrovací algoritmus reálně fungoval, před samotným použitím je nutno zakódovat otevřený text do číselné podoby. Pro to slouží funkce preved_otevreny_text, která pomocí ord() převede znak do podoby celého čísla a vrátí pole integerů.

```
def preved_otevreny_text(otevreny_text):
    pole_textu = []
    for i in otevreny_text:
        pole_textu.append(ord(i))
    return pole_textu
```

Posledním krokem k vytvoření zašifrovaného textu je převést sekvenci čísel na text. K tomu mi posloužila funkce chr(), která dokáže celočíselné hodnoty převést do znaků.

```
def preved_sifrovany_text(sifrovany_text):
    pole_textu = []
    for i in sifrovany_text:
        pole_textu.append(chr(i))
    return "".join([str(i) for i in pole_textu])
```

3.4 Analyzování výstupu

Výstupem programu je zašifrovaný text pomocí rovnice logistické mapy.

Výstup programu může být například následující:

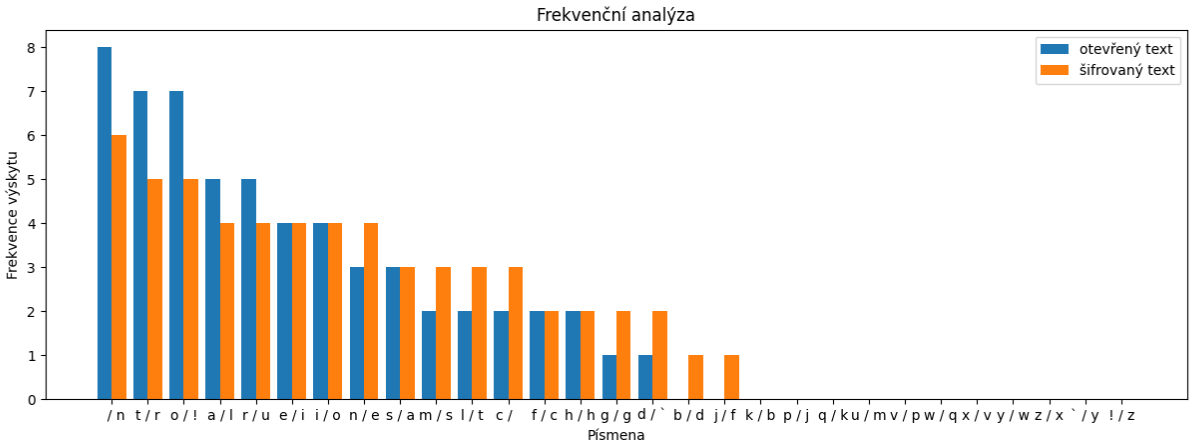
otevřený text:

material consisting of threads of cotton or other materiál

šifrovaný text:

laudrial!cnoristhng ng!uireaes!nf coutno!or nthes!l`ueri`l

Pro zkoumání a srovnání výstupu a vstupu je dobré se podívat na frekvenční analýzu. Zjistíme tedy, že frekvence výskytu písmen je naprosto odlišná v otevřeném textu a v textu zašifrovaném.



Obrázek 8 Frekvenční analýza uvedeného šifrovacího algoritmu

Na dalším příkladu je pěkné znázornění jedné z nejdůležitějších charakteristik chaosu, a to vysoká citlivost na malé počáteční změny. Nebudu nijak moct experimentovat s počátečními podmínkami, jen změním hodnotu „x“ z x=0,4 na x=0,37. Vše ostatní zůstane stejné.

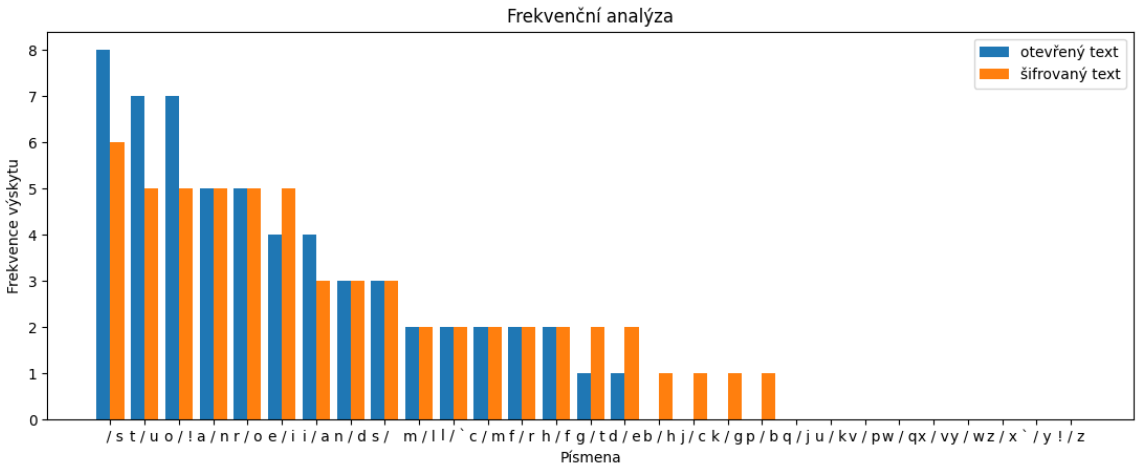
Výstup:

otevřený text:

material consisting of threads of cotton or other materiál

šifrovaný text:

laudsh`m!cnosiruiof!nf tirdaes!ng!bnutno os!ouids mauesi`l



Obrázek 9 Frekvenční analýza šifrovacího programu s pozměněným „x“

Tady je možné pozorovat odchylky v chaotickém chování a jeho dopad na proces šifrování. Zašifrovaný text je naprosto jiný a také frekvenční analýza se naprosto liší.

3.5 Popis implementace dešifrování pomocí logistické mapy

Pro dešifrování je potřeba znát klíče kterými jsme zprávu zašifrovali. Ty získáme za použití stejné funkce opakováním logistické mapy jako při šifrování se stejnými parametry „r“ a „x“. Potom jen zbývá napsat funkci „desifruj“, ve které jsem opět použila operátor XOR, který srovnal každý bit šifrového textu s odpovídajícím bitem toku klíčů.

```
def desifruj(sifrovany_text, klic):
    desifrovany_text = []
    for i in range(len(sifrovany_text)):
        desifrovany_text.append(sifrovany_text[i] ^ klic[i % len(klic)])
    return desifrovany_text
```

Výsledkem je pole čísel, které odpovídá číselnému poli otevřeného textu. Pro převedení čísel na znaky opět použiji již existující funkci, kterou jsem použila v prvním kroku při šifrování a výstupem je dešifrovaná zpráva.

ZÁVĚR

V teoretické části této práce je kladen důraz na pečlivé vysvětlení důležitých kryptografických pojmů a matematických funkcí, které se dodnes využívají. Je zde také letmo zmíněna historie deterministického chaosu a jeho využití v kryptografii. Jsou zde popsány kryptografické systémy a zmíněna jejich funkce. Bakalářská práce ukázala, že deterministický chaos má potenciál poskytnout nové přístupy v oblasti kryptografie. Chaotické systémy se vyznačují nestabilitou a citlivostí na počáteční podmínky, což znamená, že i malé změny ve vstupních hodnotách mohou mít výrazný dopad na výstupní posloupnost. Tato vlastnost je velmi cenná při vytváření bezpečných klíčů a šifrovacích postupů, jak je ukázáno v praktické části.

Při použití deterministického chaosu v kryptografii je důležité zohlednit i omezení a bezpečnostní rizika. Je nutné zajistit dostatečně dlouhou délku klíče a vhodně zvolit parametry chaotického systému, aby se minimalizovala možnost prolomení šifry. Přestože deterministický chaos přináší inovativní přístup k zabezpečení informací, další výzkum je nezbytný. Je třeba provést další analýzy a testování, aby se lépe porozumělo bezpečnostním aspektům a efektivitě použití tohoto přístupu v reálných kryptografických systémech.

SEZNAM POUŽITÉ LITERATURY

[1] Cryptography Definition. In: Kaspersky [online]. 2023, s. 1 [cit. 2023-05-25]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-cryptography

[2] SIMMONS, Gustavus J. Symmetric and Asymmetric Encryption [online]. New Mexico, 1979 [cit. 2023-05-25]. Dostupné z: https://doi.org/10.1145/356789.356793. Sandia Laboratories.

[3] Chaos: ancient Greek religion [online]. Edinburgh, Scotland: Britannica, T. Editors of Encyclopaedia, 2019 [cit. 2023-05-25]. Dostupné z: https://www.britannica.com/topic/Chaos-ancient-Greek-religion

[4] JUST a Heinz Georg SCHUSTER. Deterministic Chaos: An Introduction. 4th edition. Weinheim: WILEY-VCH Verlag GmbH & Co., 2005. ISBN 978-3-527-40415-5.

[5] DVOŘÁK, Leoš. Hamiltonovy rovnice: K přednášce NUFY028 Teoretická mechanika. Praha, 2014.

[6] Cryptography [online]. Newton, Massachusetts, United States: TechTarget, 2021 [cit. 2023-05-25]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/cryptography#:~:text=Cryptography%20is%20a%20method%20of,can%20read%20and%20process%20it

[7] APPLIED CRYPTOGRAPHY AND NETWORK SECURITY. Croatia: InTech, 2012. ISBN 978-953-51-0218-2.

[8] CIMINO, Al. Příběh kryptologie: od starověkých šifer po kvantovou kryptografii. Přeložil Marek ČTRNÁCT. Praha: Dobrovský, 2018. Knihy Omega. ISBN 9788073908874.

[9] BURDA, Karel. Úvod do kryptografie. Brno: Akademické nakladatelství CERM, 2015. ISBN 9788072049257.

[10] OULEHLA, Milan a Roman JAŠEK. Moderní kryptografie. [Praha]: IFP Publishing, 2017. ISBN 9788087383674.

[11] BUDIŠ, Petr. Elektronický podpis a jeho aplikace v praxi. Olomouc: ANAG, 2008. Právo (ANAG). ISBN 9788072634651.

[12] KALABUS, Radek. Deterministický chaos a jeho využití v kryptografii. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 47 s. Dostupné také z: http://hdl.handle.net/10563/14199. Tomas Bata University in Zlín. Faculty of Applied Informatics, Ústav aplikované informatiky. Vedoucí práce Giesl, Jiří.

[13] HORÁK, Jiří, Ladislav KRLÍN a Aleš RAIDL. Deterministický chaos a podivná kinetika. Praha: Academia, 2007. ISBN 9788020015310.

[14] HORÁK, Jiří, Ladislav KRLÍN a Aleš RAIDL. Deterministický chaos a jeho fyzikální aplikace. Praha: Academia, 2003. ISBN 9788020009104.

[15] Poincaré maps for multiscale physics discovery and nonlinear Floquet theory [online]. Amsterdam, The Netherlands: Science Direct, 2020 [cit. 2023-05-25]. Dostupné z: https://www.sciencedirect.com/science/article/abs/pii/S0167278919305470?via%3Dihub

[16] ECKERTOVÁ, Ludmila. Cesty poznávání ve fyzice. Praha: Prometheus Praha, 2004. ISBN 80-7196-293-7.

[17] Edward Lorenz [online]. Edinburgh, Scotland: T. Editors of Encyclopaedia, 2023 [cit. 2023-05-25]. Dostupné z: https://www.britannica.com/biography/Edward-Lorenz

[18] How Chaos Theory Works [online]. Atlanta, Georgia, United States: howstuffworks, 2020 [cit. 2023-05-25]. Dostupné z: https://science.howstuffworks.com/math-concepts/chaos-theory4.htm

[19] FIŠER, Jiří. Úvod do teorie obyčejných diferenciálních a diferenčních rovnic. Olomouc: Univerzita Palackého v Olomouci, 2013. ISBN 978-80-244-3401-8.

[20] BURDA, Karel. Kryptografie okolo nás. Praha: CZ.NIC, z. s. p. o, 2019. ISBN 978-80-88168-49-2.

[21] What does Entropy Measure? An Intuitive Explanation [online]. Toronto, Ontario: Towards Data Science, 2023 [cit. 2023-05-25]. Dostupné z: https://towardsdatascience.com/what-does-entropy-measure-an-intuitive-explanation-a7f7e5d16421

[22] Úvod do kryptologie. Technická univerzita v Liberci, 2021. Dostupné také z: https://elearning.tul.cz/mod/resource/view.php?id=330002&forceview=1

[23] Frekvenční analýza [online]. Opava, 2022 [cit. 2023-05-25]. Dostupné z: https://www.matweb.cz/matweb.cz/frekvencni-analyza/

[24] Frekvenční analýza [online]. 2018 [cit. 2023-05-25]. Dostupné z: https://wikisofia.cz/wiki/Frekven%C4%8Dn%C3%AD_anal%C3%BDza

[25] Atbash [online]. Praha: Univerzita Karlova v Praze, Filozofická fakulta, 2018 [cit. 2023-05-25]. Dostupné z: https://wikisofia.cz/wiki/Atbash

[26] Caesar Cipher in Cryptography [online]. Noida, Uttar Pradesh,India: GeeksForGeeks, 2023 [cit. 2023-05-25]. Dostupné z: https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/

[27] Substitution Cipher [online]. Edmonton, Alberta, Canada: Techopedia, 2018 [cit. 2023-05-25]. Dostupné z: https://www.techopedia.com/definition/9569/substitution-cipher

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES Advanced Encryption Standard

DES Data Encryption Standard

S-Box Substitution Box

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: CD-ROM

CD-ROM obsahuje program vytvořený v jazyce python a bakalářskou práci v pdf.