DHBW
Duale Hochschule
Baden-Württemberg
Mannheim

Duale Hochschule Baden-Württemberg Mannheim

Ausarbeitungen im Modul Artificial Intelligence

Studiengang Wirtschaftsinformatik

Studienrichtung Data Science

Matrikelnummer:	6699329
Firma:	Volkswagen Vertriebsbetreuungsgesellschaft mbH
Kurs:	WWI18-DSB
Kursleiter:	Prof. Maximilian Scherer
Studiengangsleiter:	Prof. Bernhard Drabant

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Quelltextverzeichnis

Algorithmenverzeichnis

Abkürzungsverzeichnis

AI	Artificial Intelligence

1 Einleitung

Diese wissenschaftliche Ausarbeitung beschäftigt sich mit Themen aus dem Bereich AI, welche im Zusammenhang mit gleichnamiger Vorlesung behandelt wurden. Dabei wird auf vier Themengebiete eingegangen:

1. Historische Entwicklung von AI
2. Gesellschaftliche Auswirkungen von AI
3. Evolutionäre und Genetische Algorithmen zur Bewältigung komplexer Aufgaben
4. Generative Verfahren der AI

Für jedes Themengebiet wird in dem jeweiligen Folgekapitel ein bestimmter Bereich oder ein Thema ausführlich erläutert, wobei es zu den letzten beiden Themen auch einen praktischen Teil gibt.

Für Thema 1 wird die historische Entwicklung im Bereich der maschinellen Entschlüsselung von Sicherheitscodes betrachtet. Dabei wird auf den ersten Meilenstein dieses Gebietes, die Enigma dechiffriere Maschine von Alan Turing geschaut und betrachtet, wie sich die Komplexität von Entschlüsselungsverfahren bis heute verändert hat.

Im Thema gesellschaftliche Auswirkungen von AI wird auf die Frage eingegangen, welche Jobs und Tätigkeiten künftig von künstlicher Intelligenz übernommen werden können und in welchem Zeitlichen Korridor dies geschehen kann. Damit verbunden wird jedoch auch aufgezeigt, wie viele neue Tätigkeitsbereiche AI der Menschheit eröffnet hat.

Der dritte Themenbereich vergleicht zwei Vorgehensweisen für das automatisierte Handeln mit Krypto Währungen. Dafür wird ein Baselinemodell Anhand eines „buy low, sell high“ Ansatzes implementiert und einem Reinforcement Learning Modell gegenübergestellt. Die beiden Modelle werden dann Anhand von Transaktionen im tatsächlichen Aktienmarkt evaluiert.

Bei den generativen Verfahren der AI wird Mithilfe des von Google DeepMind entwickelten WaveNet ein Deep Learning basiertes generatives Modell entwickelt, welches eigenständig Musik produzieren kann.Die Ergebnisse werden dann in einem Podcast über das Projekt evaluiert.

2 Historische Entwicklung der digitalen Kryptographie

Mit der Entwicklung von Computern und der damit einhergehenden Verarbeitung von Daten darf die Frage nach dem Datenschutz und der Datensicherheit nicht außer Acht gelassen werden. Analoge Daten in Form von Papier können in Tresoren und verschlossenen Koffern transportiert werden. Dieses System wurde bereits bei den Anfängen der digitalen Datenübertragung beachtet und es wurden bestimmte Sicherheiten eingebaut. Das aufbrechen dieser Verschlüsselungsmethoden ist dem Gebiet der Kryptographie zuzuordnen. In diesem Fachbereich werden Methoden entwickelt um komplexe Verschlüsselungen aufzubrechen. Die Sicherheit von Daten, die durch verteilte Systeme fließen, hat in der heutigen Gesellschaft einen hohen Wert. Dennoch ist es notwendig diese Verschlüsselungen aufbrechen zu können, um zum Beispiel bei Kriminellen Vorgängen diese frühzeitig zu unterbinden. Dafür ist es notwendig, dass die Kriminalpolizei eben solche Mittel zur Hand hat, um Verschlüsselungen bei Gefahr im Vollzug aufbrechen zu können. Mit dem kontrollierten und begründeten Aufbrechen von digitalen Verschlüsselungen kann ein höheres Sicherheitsgefühl bei der Bevölkerung gewährleistet werden.

Im weiteren Verlauf werden die einige wichtige Meilensteine der Digitalen Entschlüsselung von Codes näher dargestellt. Dabei liegt das Augenmerk auf immer komplexeren Verschlüsselungen und den damit einhergehenden komplizierteren Anwendungen, zum entschlüsseln eben dieser Codes. Die Historische Entwicklung wird dabei auf zwei Wichtige Ereignisse der Vergangenheit konzentriert und gibt weiterhin einen Blick in die Zukunft in Sachen Quantenkryptographie. Die Folgenden Meilensteine werden näher betrachtet:

- Turing - Bombe
- VENONA - Projekt
- Quantenkryptographie

Turing - Bombe

Quelle 1:

bloemer_2012

*** Zitate -direkt ***

Die Enigma war eine bereits 1918 von Arthur Scher- bius patentierte Verschlüsselungsmaschine. Sie wurde sowohl im zivilen als auch im militärischen Bereicheingesetzt.DiedeutscheReichswehr(ab19 Wehrmacht) setzte die Enigma seit 1930 ein.

Von außen betrachtet ähnelte die Enigma in allen Varianten einer großen Schreibmaschine. Al- lerdings besaß die Enigma neben der Tastatur mit den 26 Buchstaben von A bis Z noch ein Lampenfeld, bestehend aus jeweils einem Lämpchen für jeden der 26 Buchstaben. Die Anordnung der Buchstaben auf der Tastatur und dem Lampenfeld entspricht fast der noch heute üblichen Tastenordnung. Der kryptogra- fische Kern der Enigma bestand aus dem Steckerbrett und dem Walzensatz. Diese waren bei geschlossener Enigma nicht oder nur in Teilen zu sehen. Wurde die Enigma jedoch aufgeklappt (wie in Abb. 1), so waren Steckerbrett und Walzensatz zu sehen.

Die Enigma enthielt eine kleine Batterie und durch Drücken eines Buchstabens auf der Tastatur wurde ein Stromkreis geschlossen. Dieses führte zum Aufleuchten eines Buchstabens im Lampenfeld, der die Verschlüsselung des auf der Tastatur gedrückten Buchstabens war. Eine Nachricht wurde verschlüsselt, indem sukzessive die Buchstaben der Nachricht auf der Tastatur gedrückt und die danach im Lampenfeld aufleuchtenden Buchstaben notiert wurden. Die so erhaltene verschlüsselte oder chiffrierte Nachricht, der Chiffretext, wurde per Funk übertragen.

Mit jeder 26. Rotation der mittleren Walze rotierte auch die linke der inneren drei Walzen. Damit berechneten die drei inneren Walzen einer Enigma nacheinander $26 \cdot 26 \cdot 25 = 16\,900$ unterschiedliche Substitutionen und die Enigma erreichte erst nach 16 900 Buchstaben wieder ihren ursprünglichen Zustand: Eine 3-Walzen-Enigma berechnete eine polyalphabetische Substitutions Chiffre mit Blocklänge 16 900. Da die Nachrichten, die mit einer Enigma verschlüsselt wurden, deutlich kürzer als 16 900 waren, war der klassische und seit Mitte des 19. Jahrhunderts bekannte Kasiski-Angriff auf die Vigenere-Chiffre der Enigma nicht möglich. Dieses war der wesentliche Grund für das, wie sich später zeigte, nicht gerechtfertigte Vertrauen der Wehrmacht und der deutschen Geheimdienste in die Sicherheit der Enigma. *** hier sollte man vielleicht noch ein wenig ausholen, was die walzen und so betrifft, dass man auch ein wenig versteht was da vor sich geht

Die deutschen Streitkräfte und Geheimdienste wa- ren bis zum Ende des Zweiten Weltkriegs von der Sicherheit der Enigma überzeugt. Ihnen war zwar bewusst, dass die Alliierten immer

wieder geheime deutsche Informationen kannten, doch sie erklärten dies vornehmlich durch Spionage und Verrat. Die Alliierten konnten jedoch ab 1941 mit einer Unter- brechung von Februar 1942 bis etwa November 1942 einen Großteil des Enigma-Nachrichtenverkehrs abhören. Entscheidend hierfür waren, neben den oben erwähnten Besonderheiten der Enigma, vor allem 1. geniale Köpfe, insbesondere natürlich Alan Turing selbst, 2. brillanteIdeenundclevereAngriffe, 3. speziell konstruierte Maschinen, die Turing- Welchman-Bomben, die einen Großteil des Codebrechens automatisierten, 4. Entwurfsfehler, wie die beiden oben genannten Besonderheiten der Enigma, 5. unsichere Bedienung und Nutzung der Enigma, insbesondere schlechtes Schlüsselmanagement und 6. (Kriegs-)Glück, zum Beispiel das Aufbringen von U-Booten mit unversehrten Enigma-Maschinen und Schlüsselbüchern.

In der Sprache heutiger Kryptografie ausgedrückt, benutzten die Codebrecher von Bletchley Park Angriffe mit bekannten oder gewählten Klartexten, um die Tagesschlüssel einer Enigma in- nerhalb weniger Stunden zu berechnen. Die Idee selber stammte nicht von Turing, sie wurde vielmehr schon von polnischen Codebrechern um Marian RejewskiindenJahrenunmittelbarvorAusbruch des Zweiten Weltkriegs entwickelt. Die polnischen Mathematiker hatten im Juli 1939 ihre Kenntnisse der Enigma und ihrer Schwächen an britische und französische Geheimdienstler übergeben. Es war Alan Turing, der das volle Potenzial ihrer Ideen erkannte und sie perfektionierte.

Die Idee eines Angriffs mit bekannten Klartexten ist leicht zu erklären. Die von den deutschen Streitkräften und Geheimdiensten mit der Enigma verschlüsselten Nachrichten enthielten viele immer wieder auftauchende Fragmente. So enthielten chiffrierte Nachrichten häufig Wetterberichte mit bekannten, häufig wiederkehrenden Schlagworten. Diese Textfragmente nannten die Codebrecher von Bletchley Park Cribs1 . Kannte man ein Crib und seine genaue Position in einer Nachricht, versuchte man, diejenigen Schlüssel zu bestimmen, die aus dem Crib den entsprechenden Teil des Chiffretextes erzeugten. Unter den (hoffentlich) wenigen gefundenen Kandidaten wurden schließlich, durch Probieren, Teile des Tagesschlüssels, insbesondere die Walzenlage, ermittelt.

Leider können wir hier nicht auf die vielfältigen zusätzlichen Ideen und Tricks eingehen, mit denen die Codebrecher um Alan Turing ab Mai 1941 den Tagesschlüssel der von der Marine eingesetzten 3-Walzen-Enigma in der Regel innerhalb weniger Stunden berechneten. Im Februar 1942 wechselte die deutsche Marine jedoch zu einer 4-Walzen-Enigma. Bis auf einige wenige Tage konnten die Codebrecher von Bletchley Park bis Dezember 1942 diese Variante der Enigma nicht knacken. Durch viel Glück (am 30.10.1942 wurde ein deutsches U-Boot mit intakter Enigma und Schlüsselbuch vor Port Said aufgebracht), Ungeschick

auf deutscher Seite (für Wetterberichte wurde die 4-Walzen-Enigma als 3-Walzen-Enigma mit eingeschränktem Tagesschlüssel eingesetzt) und durch verbesserte Hardware (die britischen Bomben wurden durch leistungsfähigere amerikanische Bomben ersetzt), konnten ab Dezember 1942 auch die Tagesschlüssel der 4-Walzen-Enigma der Marine wieder innerhalb weniger Stunden berechnet werden.

Die Alliierten setzten alles daran, die Sicherheit ihrer Versorgungskonvois zu garantieren, daher lässt eine solche Statistik die Bedeutung von Bletchley Park für die alliierten Kriegsanstrengungen und den Verlauf des Zweiten Weltkriegs zumindest erahnen.

Quelle 2: **oepen_hoefer_2007**

*** Zitate -direkt ***

Die Geschichte der Entschlüsselung der Enigma lässt sich in zwei Phasen aufteilen. Vor dem Krieg sind vor allem die Leistungen der Polen hervorzuheben. Nach der Besetzung Polens durch die Deutschen wurde die Arbeit der polnischen Kryptoanalytiker von den Briten fortgesetzt.

Einige Jahre lang entschlüsselten die polnischen Kryptoanalytiker den deutschen Nachrichtenverkehr erfolgreich. Doch als die Deutschen 1926 die Enigma einführten, gelang ihnen das nicht mehr

Um geeignete Kryptoanalytiker mit mathematischer Ausbildung zu finden, veranstaltete er an der Universität Posen einen Kryptographiewettbewerb, bei welchem er drei Mathematiker für die Arbeit im Biuro Szyfrow auswählte. Tatsächlich wählte Ciezki die Universität Posen aus, da diese vor dem ersten Weltkrieg noch in deutscher Hand gewesen war, und somit die meisten Studenten und Lehrenden der Universität fließend Deutsch sprachen. Der begabteste der drei ausgewählten Mathematiker war Marian Rejewski. Dieser wurde sogleich mit der Entschlüsselung der Enigma beauftragt. Hierfür standen ihm zunächst nur eine kommerzielle Variante der Enigma und die bisher abgefangenen verschlüsselten Nachrichten der Deutschen zur Verfügung. Die kommerzielle Variante der Enigma unterschied sich jedoch signifikant von der militärischen Variante, da sie zum einen nicht über ein Steckbrett verfügte und zum anderen ihre Walzen anders verdrahtet waren. Rejewski versuchte zunächst die interne Walzenverdrahtung der militärischen Enigma zu ergründen. Es gelang ihm eine Gleichung aufzustellen, aus welcher die Walzenverdrahtung berechnet werden konnte. Allerdings enthielt die- se Gleichung noch zu viele Unbekannte, um sie zu lösen.

Walzen IV und V zu erschließen, jedoch stieg die Anzahl der möglichen Walzenpositionen nun von 6 auf 60 (5, statt 3 Möglichkeiten). Um diese neue Variante der Enigma zu entschlüsseln, 3 wären somit 60 statt 6 Bombas notwendig gewesen. Den Polen fehlten das Material und die Zeit um die Enigma ein weiteres Mal zu entschlüsseln. Als klar wurde, dass es bald zu einer deutschen Invasion in Polen kommen wu rde, beschlossen die Polen ihre Forschungsergebnisse an die Alliierten weiterzugeben.

VENONA - Projekt

simkin_2020 In 1942 the United States Army's Signals Intelligence Service recruited Meredith Gardner to work on breaking German codes. During this period he also taught himself Japanese so that he could also work on their codes as well. He spent the rest of the war studying messages between Germany and Japan. "He worked initially on German ciphers and then on Japanese super-enciphered codes, in which messages were first encoded in five-figure groups taken from a code book and then enciphered by adding a series of randomly produced figures, known as an additive, which was taken from a second book."(1) After the war Gardner was assigned to help decode a backlog of communications between Moscow and its foreign missions. By 1945, over 200,000 messages had been transcribed and now a team of cryptanalysts attempted to decrypt them. The project, named Venona (a word which appropriately, has no meaning), was based at Arlington Hall, Virginia. (2) Soviet messages were produced in exactly the same way as Japanese super-enciphered codes. However, "where the Japanese gave the codebreakers a way in by repeatedly using the same sequences of additive, the Russian system did not. As its name suggests, the additive appeared on separate sheets of a pad. Once a stream of additive had been used, that sheet was torn off and destroyed, making the message impossible to break."(3)

venona_NSA The U.S. Army's Signal Intelligence Service, the precursor to the National Security Agency, began a secret program in February 1943 later codenamed VENONA. The mission of this small program was to examine and exploit Soviet diplomatic communications but after the program began, the message traffic included espionage efforts as well. Although it took almost two years before American cryptologists were able to break the KGB encryption, the information gained through these transactions provided U.S. leadership insight into Soviet intentions and treasonous activities of government employees until the program was canceled in 1980. The VENONA files are most famous for exposing Julius (code named LIBERAL) and Ethel Rosenberg and Reealing give indisputable evidence of their involvement with the Soviet spy ring. The first of six public releases of translated

VENONA messages was made in July 1995 and included 49 messages about the Soviets' efforts to gain information on the U.S. atomic bomb research and the Manhattan Project. Over the course of five more releases, all of the approximately 3,000 VENONA translations were made public.

Quantenkryptographie

tittel_brendel_gisin_ribordy_zbinden_1999 Quantenkryptographie in der PraxisAlle bisherigen Experimente verwendeten Photonenals Informationsträger. Sie sind experimentell relativeinfach zu erzeugen und lassen sich mit Hilfe vonGlasfasern transportieren, eine Technik, die innerhalbder letzten Jahrzehnte, bedingt durch die enorme Ex-pansion der Telekommunikation, große Fortschritte zuverzeichnen hat.

Quantenkryptographie, die am weitesten entwickel-te Anwendung des neuen Gebietes der Quantenkom-munikation, hat seit vier Jahren das Labor verlassen.Experimente unter realen Bedingungen sind, zumindestwas Systeme angeht, die auf Kodierung mit „schwa-chen Pulsen“ beruhen, heutzutage schon fast eine Routineübung. Reichweiten liegen in der Gegend von20 – 30 Kilometern, und Quantenbit-Fehlerraten vonwenigen Prozent sind niedrig genug, um einenLauschangriff detektieren und die sichere Übertragungeines Schlüssels gewährleisten zu können. Somit kön-nen existierende System schon heute eine sichereÜbertragung von Nachrichten garantieren, falls Verfah-ren, die auf mathematischer Komplexität beruhen, „ge-knackt“ werden sollten.

rass_schartner_2002 Quantenkryptographie gilt als Schlusseltechnologie der kommenden Jahrzehnte. Uber 20 Jahre hat die Evolution von der Idee bis zu den ersten Prototypen gedauert, die bereits heute demonstrieren, dass zukunftige Netzwerke mit hoher Sicherheit optisch sein werden.

Anders sieht die Situation im Umfeld der Quantencomputer aus. Peter Shor hat 1997 zwei Algorithmen veroffentlicht, welche das Faktorisierungsproblem und das diskrete Logarithmus-Problem auf einem Quantencomputer effizient losen [20]. Unterstellt man den Quantencomputern eine ahnliche Evolution wie den heutigen PCs, so erscheint eine Massen- fertigung von Quantencomputern in den kommenden Jahrzehnten keineswegs un- plausibel, womit zumindest die sicher- heitsrelevanten Grundannahmen vieler asymmetrischen kryptographischen Ver- fahren nicht langer haltbar waren.

Existiert ein Ubertragungsmedium, welches nicht ko- pierbar ist? Eine positive Antwort hierauf wurde 1982 von Wootters und Zurek ge- geben [25], und von Steven Wiesner in ei- nem uber mehr als zehn Jahre unverof- fentlichten Manuskript aufgegriffen [24]. Diese innovative Idee wurde von Bennett und Brassard weiterentwickelt zu dem, was wir heute als quantenkryptographi- schen Schlusselaustausch (QKD – quan- tum key distribution) kennen. Die Grundidee ist einfach: Anstatt Bits auf elektromagnetische Impulse zu modulieren, findet eine Codierung in Form von polarisierten Photonen statt. Diese kon- nen nach den Ergebnissen von Wootters und Zurek nicht storungsfrei kopiert wer- den [25]. Damit fuhrt jeder Abhorversuch unweigerlich zu einem unnaturlichen An- stieg der Fehlerrate uber das durch unver- meidliche Messfehler verursachte Ausmaß hinaus. Dieser Anstieg kann an beiden En- den des Kanals erkannt werden und zum sofortigen Abbruch der Kommunikation fuhren.

Der technologische Fortschritt in der Entwicklung der Gerate lasst jedoch er- warten, dass in naher Zukunft ausrei- chend hohe Bitraten fur eine One-Time Pad-Verschlusselung zur Verfugung ste- hen. Wahrend dieser Umstand lediglich eine Einschrankung, aber keine Gefahr im eigentlichen Sinne darstellt, sind tatsachli- che Angriffe auf QKD Kanale bei Einsatz von nicht-vertrauenswurdiger Hardware durchaus denkbar. Eine Reihe von Losungsvorschlagen fur dieses Problem wurde im Laufe der Jahre erarbeitet. Darunter Ansatze uber Mehrwege-Ubertragung [16, 23], theoretische Betrachtungen von Kanalen mit „unbe- schrankter“ Lange [14] und Sicherheits- analysen von Systemen mit nicht-vertrau- enswurdiger Hardware [1]. Die Zukunft wird zeigen, welche Ansatze sich als prak- tikabel erweisen und durchsetzen werden.

Fazit

*** Fazit *** - was sind die performantesten systeme heute? - oder ist der Brute Force immer noch der Effektivste

- Was ist am Spruch dran, "Der beste Code ist nur so sicher so lange es keinen schnelleren Computer auf der Welt gibt, der diesen code schneller Knacken kann als er wieder erneuert wird

3 Gesellschaftliche Auswirkungen von AI

Welche Jobs und Tätigkeiten werden künftig von AI übernommen und wie lange dauert das in bestimmten Fällen noch? Wie schnell werden Computer uns im Leben ersetzen und in welchen Bereichen ist das schon geschehen?

4 Evolutionäre und Genetische Algorithmen zur Bewältigung komplexer Aufgaben

Vergleich zweier Crypto Trading bots, zum einen Regelbasiert (Buy low, sell high) und eines Reinformcement learnings zum Automatisierten Aktienhandel. Diese Thematik wird implementiert und dann im Umfang einer Präsentation in der Vorlesung vorgetragen und wissenschaftlich dokumentiert.

5 Generative Verfahren der AI

Anhand von WaveNet, einem Deep Learning basierten generativen Model entwickelt von Google DeepMind soll Musik produziert werden. Das Ziel dabei ist anhand von liedern verschiedener Künstler (seiner lieblingskünstler) neue Musik zu creieren, damit man nicht immer das gleiche hören muss. Die Ergebnisse werden dann entweder in einer Präsentation während der Vorlesung oder in einem kurzen Podcast vorgestellt und Bewertet.

6 Zusammenfassung der Forschungsthemen