KRYPTOLOGIE UND SYSTEMSICHERHEIT

Sommersemester 2020

Technische Hochschule Mittelhessen

Andre Rein

– Historische Kryptographische Verfahren –

VERSCHIEBE- ODER CAESAR-CHIFFRE

- Die klassische Caesar-Chiffre ist eine bestimmte Form einer monoalphabetischen Substitution
- Es erfolgt aber hierbei nur eine **Verschiebung** um x Positionen des Alphabets
  - z.B. (A → D), (B → E), (C → F), …, (X → A),(Y → B),(Z → C)
- Es handelt sich also um eine Verschiebung der Buchstaben → Daher **Verschiebechiffre**

VERSCHIEBE- ODER CAESAR-CHIFFRE

Die Buchstaben des Alphabets können hierbei als Elemente des Restklassenrings $\mathbb{Z}_{26}$ aufgefasst werden.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	2

Verschiebechiffre

Es seien $x, y, z \in \mathbb{Z}_{26}$.

- **Verschlüsselung**: $e_k(x) \equiv x + k \bmod 26$
- **Entschlüsselung**: $d_k(y) \equiv y - k \bmod 26$

CAESAR VER/ENTSCHLÜSSELUNG ✍

- Verschlüsseln Sie den Text `ATTACK`, bei gegebenen Schlüssel $k = 13$
- Entschlüsseln Sie den Text `RK URNE`, bei gegebenen Schlüssel $k = 17$

Dauer: 10 Minuten

CAESAR-CHIFFRE - KRYPTOANALYSE

Die Caesar-Chiffre lässt sich, genau wie die monoalphabetische Substitution, mittels Häufigkeitsanalyse brechen.

Frage: Wie viele möglichen Schlüssel gibt es bei einer einfachen Verschiebechiffre im lateinischen Alphabet und kann man diese Variante mittels Brute Force brechen?

CAESAR-CHIFFRE - BRUTE FORCE

```
  Beispieltext: GlhFdhvduFkliiuhlvwvhkuhlqidfkcxeuhfkhq
Brute Force 01: FkgEcguctEjkhhtgkuvugjtgkphcejbwdtgejgp
            02: EjfDbftbsDijggsfjtutfisfjogbdiavcsfdifo
            03: DieCaesarChiffreistsehreinfachzubrechen
            04: ChdBzdrzqBgheeqdhrsrdgqdhmezbgytaqdbgdm
            05: BgcAycqypAfgddpcgqrqcfpcgldyafxszpcafcl
            06: AfbZxbpxoZefccobfpqpbeobfkcxzewryobzebk
            07: ZeaYwaownYdebbnaeopoadnaejbwydvqxnaydaj
            08: YdzXvznvmXcdaamzdnonzcmzdiavxcupwmzxczi
            09: XcyWuymulWbczzlycmnmyblychzuwbtovlywbyh
            10: WbxVtxltkVabyykxblmlxakxbgytvasnukxvaxg
            11: VawUswksjUzaxxjwaklkwzjwafxsuzrmtjwuzwf
            12: UzvTrvjriTyzwwivzjkjvyivzewrtyqlsivtyve
            13: TyuSquiqhSxyvvhuyijiuxhuydvqsxpkrhusxud
            14: SxtRpthpgRwxuugtxhihtwgtxcuprwojqgtrwtc
            15: RwsQosgofQvwttfswghgsvfswbtoqvnipfsqvsb
            16: QvrPnrfnePuvsservfgfruervasnpumhoerpura
            17: PuqOmqemdOturrdquefeqtdquzrmotlgndqotqz
            18: OtpNlpdlcNstqqcptdedpscptyqlnskfmcpnspy
            19: NsoMkockbMrsppboscdcorbosxpkmrjelbomrox
            20: MrnLjnbjaLqrooanrbcbnqanrwojlqidkanlqnw
            21: LqmKimaizKpqnnzmqabampzmqvnikphcjzmkpmv
            22: KplJhlzhyJopmmylpzazloylpumhjogbiyljolu
            23: JokIgkygxInollxkoyzyknxkotlginfahxkinkt
            24: InjHfjxfwHmnkkwjnxyxjmwjnskfhmezgwjhmjs
            25: HmiGeiwevGlmjjvimwxwilvimrjegldyfviglir
```

AFFINE CHIFFRE

Die mathematische Form der Caesar-Chiffre war für die Verschlüsselung definiert als $e_k(x) \equiv x + k \bmod 26$ und die Entschlüsselung als $d_k(y) \equiv y - k \bmod 26$.

Affine Chiffre

Es seien $x, y, a, b \in \mathbb{Z}_{26}$.

- **Verschlüsselung**: $e_k(x) = y \equiv a * x + b \bmod 26$
- **Entschlüsselung**: $d_k(y) = x \equiv a^{-1} * (y - b) \bmod 26$

mit dem Schlüssel $k = (a, b)$, wobei gelten muss, dass $ggT(a, 26) = 1$.

	Die Caesar-Chiffre ist also eine Variante der allgemeineren affinen Chiffre, wobei $a = 1$ gilt.

AFFINE CHIFFRE - MULTIPLIKATIVE INVERSE

Der Wert a, der zur Multiplikation verwendet wird, darf nicht beliebig sein, da $ggT(a, 26) = 1$ gelten muss. In der Menge $\mathbb{Z}_{26}$ gibt es insgesamt 12 Elemente, die diese Eigenschaft erfüllen.

Berechnung mit Eulerscher Phi-Funktion: $\varphi(26) = \varphi(2) * \varphi(13) = 1 * 12$

https://de.wikipedia.org/wiki/Eulersche_Phi-Funktion

$a \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ $\rightarrow$ a darf nur diese Werte annehmen!

Modular Inverse in $\mathbb{Z}_{26}$

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

AFFINE CHIFFRE - VERSCHLÜSSELUNG

`ATTACK AT DAWN` = `0, 19, 19, 0, 2, 10, 0, 19, 3, 0, 22, 13`

$$k(a,b) = (3,5), e_k(x) \equiv a * x + b \bmod 26$$

$e_k(0) \equiv 3 * 0 + 5 \bmod 26 \equiv 5 \bmod 26$ = `F`

$e_k(19) \equiv 3 * 19 + 5 \bmod 26 \equiv 62 \bmod 26 \equiv 10 \bmod 26$ = `K`

...

Aufgabe: Berechnen Sie die restlichen Werte!✍

Dauer: 10 Minuten

AFFINE CHIFFRE - SCHLÜSSELRAUM

Frage: Wie viele möglichen Schlüssel gibt es bei einer affinen Chiffre im lateinischen Alphabet und kann man diese Variante mittels Brute Force brechen?

VIGENÈRE-CHIFFRE (EINFACHE POLYALPHABETISCHE SUBSTITUTION)

- Die Vigenère-Chiffre (1585, Blaise de Vigenère) verwendet ein sog. Schlüsselwort um einen Text zu verschlüsseln
  - z.B. `ABC`
- Wurde in der damaligen Zeit als: „le chiffre indéchiffrable“ („die unentzifferbare Chiffre“) bezeichnet
- Das Schlüsselwort bestimmt hierbei die Cäsar-Verschiebung an der jeweiligen Position
  - Da mehr als ein Alphabet zur Verschlüsselung herangezogen wird, spricht man hier von **polyalphabetisch**

VIGENÈRE-CHIFFRE

- **Verschlüsselung**:

```
dasisteinbeispiel   Plaintext
ABCABCABCABCABCAB   Schlüssel
------------------
DBUITVEJPBFKSQKEM   Ciphertext
```

- **Entschlüsselung**:

```
DBUITVEJPBFKSQKEM  Ciphertext
ABCABCABCABCABCAB  Schlüssel
------------------
dasisteinbeispiel  Plaintext
```

VIGENÈRE-QUADRAT

		Plaintext																								
			A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
		A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
		B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
		C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
		D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
		E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
		F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
S		G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
C		H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
H		I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
L		J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
Ü		K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
S		L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
S		M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
E		N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
L		O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
		P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
		Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
		R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
		S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
		T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
		U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
		V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
		W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
		X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
		Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
		Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

KRYPTOANALYSE: VIGENÈRE-CHIFFRE

- Da ein einzelner Buchstabe des Plaintexts auf verschiedene Buchstaben im Ciphertext abgebildet werden kann (je nach seiner Position), werden die statistischen Eigenschaften verwischt.
  - Man kann also nicht mehr **direkt** mit einer Häufigkeitsanalyse arbeiten!
- Man muss im Prinzip 2 Probleme lösen:
  1. Aus wie viel Einzelbuchstaben besteht das Schlüsselwort
  2. Welche Buchstaben wurden verwendet

KRYPTOANALYSE: VIGENÈRE-CHIFFRE

- Nehmen wir an, wir kennen die **länge** des Schlüsselwortes $l = 3$

```
DBUITVEJPBFKSQKEM |  Ciphertext
.-.-.-.-.-.-.-.-.- Aufteilung
v v v v v v

D I E B S E
B T J F Q M
U V P K K
```

KRYPTOANALYSE: VIGENÈRE-CHIFFRE

- Durch Ausprobieren können wir alle Möglichen Verschiebungen auf Korrektheit testen.

Test `AAA` → Falsch

```
D I E B S E  <- Verschiebung um 0 Positionen (A)
B T J F Q M  <- Verschiebung um 0 Positionen (A)
U V P K K    <- Verschiebung um 0 Positionen (A)
```

Test `ABB` → Falsch

```
D I E B S E  <- Verschiebung um 0 Positionen (A)
A S I E P L  <- Verschiebung um 1 Positionen (B)
T W N J J    <- Verschiebung um 1 Positionen (B)
```

...

Test `ABC` → Korrekt

```
D I E B S E  <- Verschiebung um 0 Positionen (A)
A S I E P L  <- Verschiebung um 1 Positionen (B)
S T N I I    <- Verschiebung um 2 Positionen (C)
```

KRYPTOANALYSE: VIGENÈRE-CHIFFRE

Typischerweise ist die Schlüsselwortlänge nicht bekannt

- Eine Auswahl an möglichen Schlüsselwortlänge kann anhand des sog. kasiski-test)
- Hierbei wird nach Bi/Tri/Tetragrammen gesucht die eine gleiche Verschiebung aufweisen
- Mittels Primfaktorzerlegung lassen sich Kandidaten der Schlüsselwortlänge bestimmen
    - *Bei Interesse lesen Sie sich in die Details ein*

	Auch mit modernen Computern können wir nicht einfach alle möglichen Kombinationen ausprobieren wenn die Schlüssellänge lang genug ist. Daher beschränkt sich die Häufikeitsanalyse auf Bi/Tri/Tetragrammen, was eine quadratische Laufzeit des Algorithmus bedeutet.

POLYALPHABETISCHE SUBSTITUTION

Bei einer vollständigen polyalphabetischen Substitution erfolgt keine Verschiebung, sondern echte frei gewählte Ersetzungen

- D.h. je nach Position eines Buchstabes wird er durch einen anderen vorgewählten Buchstaben ersetzt
- Dabei kann z.B. im **ersten Schritt** ein `B` an **Position 1** von einem beliebigen anderen Buchstaben ersetzt werden, z.B. `K`
- Und im **zweiten Schritt** ein `B` an **Position 2** durch einen beliebigen anderen Buchstaben, der in keiner Beziehung zur Ersetzung des *ersten Schritts* steht, ersetzt werden, z.B. `J`

POLYALPHABETISCHE SUBSTITUTION

Alternativ kann auch eine mehrfache Substitution hintereinander ausgeführt werden

- Z.B. im **ersten Schritt** ein `B` an **Position 1** von einem beliebigen anderen Buchstaben ersetzt werden, z.B. `K`
- Und im **zweiten Schritt** das temporär ersetzte `K` durch einen beliebigen anderen Buchstaben, der in keiner Beziehung zur Ersetzung des *ersten Schritts* steht, ersetzt werden, z.B. `X`

	Das war das Grundprinzip der Enigma Verschlüsselungsmaschine

ENIGMA

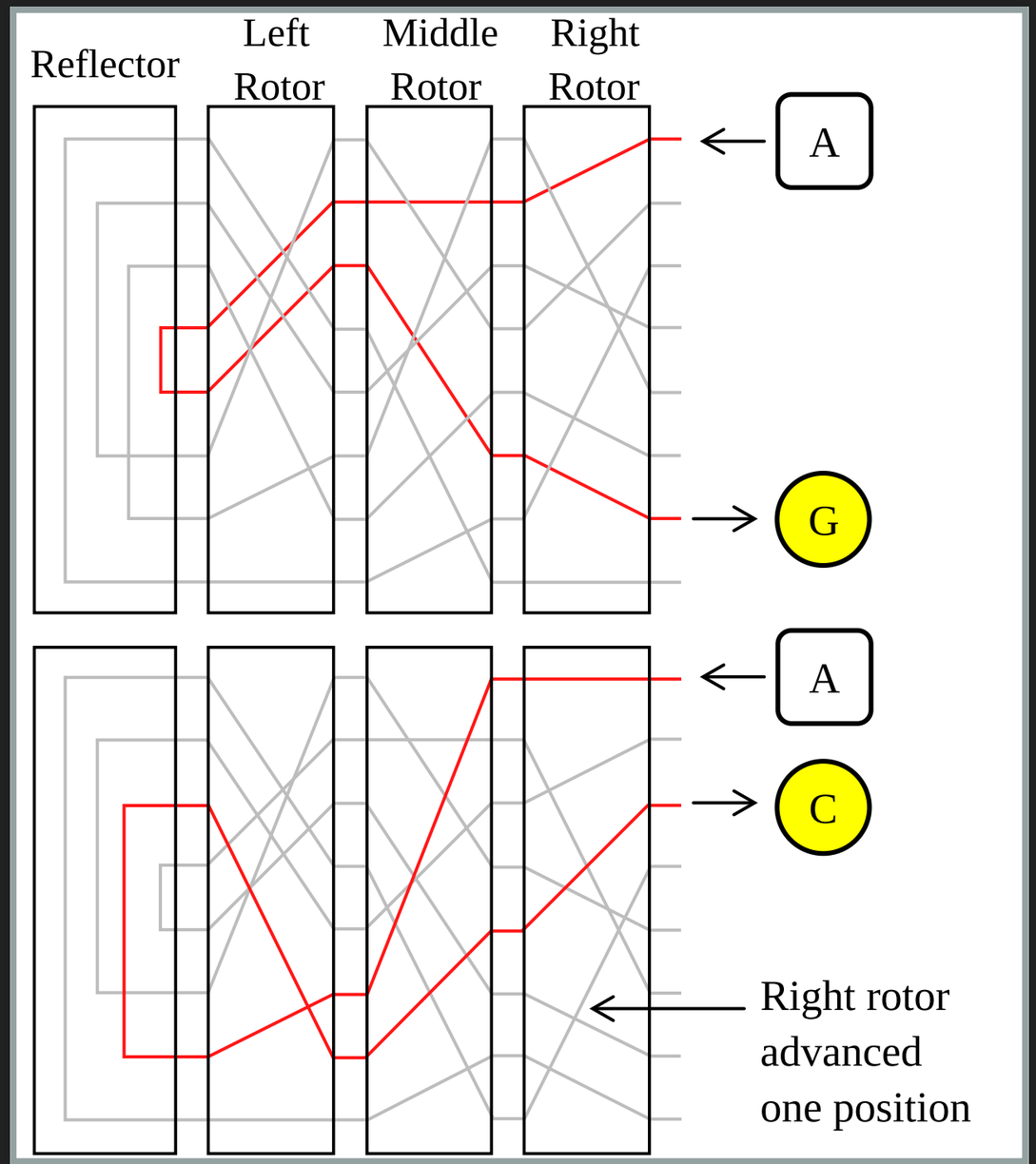
Bei der folgenden Tabelle handelt es sich um die Anordnung der Buchstaben auf den 5 Walzen der ENIGMA-I

- Die Grundfunktionalität der ENIGMA, basierte auf eine polyalphabetischen Substitution
- Die Walzenpositionen wurden jeden Tag getauscht und konnten eine initiale Rotation aufweisen (Anfangsstellung).
- Umkehrwalze war fast immer `UKW B`

```
        A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Walzen: ---------------------------------------------------
I       E K M F L G D Q V Z N T O W Y H X U S P A I B R C J
II      A J D K S I R U X B L H W T M C Q G Z N P Y F V O E
III     B D F H J L C P R T X V Z N Y E I W G A K M U S Q O
IV      E S O V P Z J A Y Q U I R H X L N F T G K D C M W B
V       V Z B R G I T Y U P S D N H L X A W M J Q O F E C K

Umkehr:-----------------------------------------------------
UKW A   E J M Z A L Y X V B W F C R Q U O N T S P I K H G D
UKW B   Y R U H Q S L D P X N G O K M I E B F Z C W V J A T
UKW C   F V P J I A O Y E D R Z X W G C T K U Q S B N M H L
```

ENIGMA



Quelle: wikipedia

ENIGMA FRAGE

Sehen Sie sich die Abbildung auf der vorherigen Folie an und beantworten Sie die Frage. Sie können sich gerne mit Ihren Kommilitonen austauschen / diskutieren.

- Wie funktioniert die Entschlüsselung bei der Enigma?

ENIGMA

Die Walzen bewegen sich mit unterschiedlicher Rotationsgeschwindigkeit und man kann einen Buchstaben bestimmten, bei dem eine Rotation der nächst langsameren Walze vorgenommen wird.

- Rechte Walze rotiert eine Position bei jedem Tastendruck
- Mittlere Walze nach max. 26 Tastendrücken
- Linke Walze nach max. 26^2 Tastendrücken
- Außerdem gab es noch Steckverbindungen, die eine Eingangspermutation der Buchstaben ermöglichte

ENIGMA

Beispiel eines Aufbaus der täglich gewechselt wurde.

Tag	Walzenlage	Ringstellung	---- Steckerverbindungen ----
31	III I IV	01 17 22	AH BL CX DI ER FK GU NP OQ TY
30	II V I	18 24 11	BN DZ EP FX GT HW IY OU QV RS
29	I IV III	16 26 08	AD CN ET FL GI JV KZ PU QY WX

ENIGMA

- Außer den hier vorgestellten Mechanismen, gibt es noch weitere Besonderheiten
- Bei Interesse an der Thematik und der Kryptoanalyse kann der Artikel in Wikipedia empfohlen werden, der sehr ausführlich ist.

ENIGMA

AUFGABEN: KRYPTOANALYSE CAESAR UND VIGENÈRE ✍

Bearbeiten Sie die Aufgaben CAESAR und VIGENERE

⏱ Bearbeitung: Rest der Stunde + Hausaufgabe :) Besprechen wir das nächste mal!