UNIVERSITÄT BAYREUTH

Kryptographie-Labor

Steffen Müller, Gerold Grünauer

4.Tag der Mathematik

Bayreuth, 11.07.2009

UNIVERSITÄT BAYREUTH

Was ist Kryptographie?

Kryptographie:

- Wissenschaft der Verschlüsselung von Information
- Verschlüsseln - Entschlüsseln – Entziffern (Knacken)

UNIVERSITÄT BAYREUTH

Was ist Kryptographie?

Kryptographie:

- Wissenschaft der Verschlüsselung von Information
- Verschlüsseln - Entschlüsseln – Entziffern (Knacken)

Früher vor allem verwendet durch:

- Militär
- Geheimdienste

UNIVERSITÄT BAYREUTH

Kryptographie heute

Wo wird heute im täglichen Leben verschlüsselt?

UNIVERSITÄT BAYREUTH

Kryptographie heute

Wo wird heute im täglichen Leben verschlüsselt?

- Bankgeschäfte im Internet (Onlinebanking)

UNIVERSITÄT BAYREUTH

Kryptographie heute

Wo wird heute im täglichen Leben verschlüsselt?

- Bankgeschäfte im Internet (Onlinebanking)
- Einkaufen im Internet bei ebay, Amazon, …

UNIVERSITÄT BAYREUTH

Kryptographie heute

Wo wird heute im täglichen Leben verschlüsselt?

- Bankgeschäfte im Internet (Onlinebanking)
- Einkaufen im Internet bei ebay, Amazon, …
- Mobiltelefone

UNIVERSITÄT BAYREUTH

Kryptographie heute

Wo wird heute im täglichen Leben verschlüsselt?

- Bankgeschäfte im Internet (Onlinebanking)
- Einkaufen im Internet bei ebay, Amazon, …
- Mobiltelefone
- Digitale Unterschrift

UNIVERSITÄT BAYREUTH

Kryptographie heute

Wo wird heute im täglichen Leben verschlüsselt?

- Bankgeschäfte im Internet (Onlinebanking)
- Einkaufen im Internet bei ebay, Amazon, …
- Mobiltelefone
- Digitale Unterschrift
- Geldautomaten

UNIVERSITÄT BAYREUTH

Folgen misslungener Verschlüsselung

1. Einkaufen mit fremden ebay-Accounts:

Platz 1: Motoryacht	**5,5 Mio €**
Platz 2: Flugzeug	**1,4 Mio €**

[Die Zeit]

UNIVERSITÄT BAYREUTH

Folgen misslungener Verschlüsselung

1. **Einkaufen mit fremden ebay-Accounts:**

   Platz 1: Motoryacht **5,5 Mio €**

   Platz 2: Flugzeug **1,4 Mio €**

   [Die Zeit]

2. **Internetkäufe mit fremder Kreditkarte:**

   Platz 1: 3 Amerikaner ergaunerten **230 Mio $**

   [New York Times]

UNIVERSITÄT BAYREUTH

Folgen misslungener Verschlüsselung

1. **Einkaufen mit fremden ebay-Accounts:**
   Platz 1: Motoryacht **5,5 Mio €**
   Platz 2: Flugzeug **1,4 Mio €**
   [Die Zeit]

2. **Internetkäufe mit fremder Kreditkarte:**
   Platz 1: 3 Amerikaner ergaunerten **230 Mio $**
   [New York Times]

3. **Betrug im Onlinebanking:**
   Schaden pro Jahr in Deutschland: **19 Mio €**
   [Die Welt]

UNIVERSITÄT BAYREUTH

Folgen misslungener Verschlüsselung

1. **Einkaufen mit fremden ebay-Accounts:**
   Platz 1: Motoryacht **5,5 Mio €**
   Platz 2: Flugzeug **1,4 Mio €**
   [Die Zeit]

2. **Internetkäufe mit fremder Kreditkarte:**
   Platz 1: 3 Amerikaner ergaunerten **230 Mio $**
   [New York Times]

3. **Betrug im Onlinebanking:**
   Schaden pro Jahr in Deutschland: **19 Mio €**
   [Die Welt]

→ Schaden vermeiden durch Kryptographie

UNIVERSITÄT BAYREUTH

Was ist Kryptographie? Teil 2

1. **Verschlüsseln:**

   Klartext mittels Geheimalphabet unleserlich machen

UNIVERSITÄT BAYREUTH

Was ist Kryptographie? Teil 2

1. **Verschlüsseln:**

   Klartext mittels Geheimalphabet unleserlich machen

2. **Entschlüsseln:**

   Empfangenen Geheimtext mit Geheimalphabet leserlich machen

UNIVERSITÄT BAYREUTH

Was ist Kryptographie? Teil 2

1. **Verschlüsseln:**
   Klartext mittels Geheimalphabet unleserlich machen
2. **Entschlüsseln:**
   Empfangenen Geheimtext mit Geheimalphabet leserlich machen
3. **Entziffern / Code knacken:**
   Abgefangenen Text ohne Geheimalphabet lesbar machen

UNIVERSITÄT BAYREUTH

Überblick

1. Klassische Verfahren:

a) Cäsar-Chiffre

→ 1. Praxisteil: Knacken von Cäsar-Codes

UNIVERSITÄT BAYREUTH

Überblick

1. **Klassische Verfahren:**
   a) Cäsar-Chiffre
      → 1. Praxisteil: Knacken von Cäsar-Codes
   b) Vigenère-Chiffre
      → 2. Praxisteil: Knacken von Vigenère-Codes

UNIVERSITÄT BAYREUTH

Überblick

1. **Klassische Verfahren:**
   a) Cäsar-Chiffre
      → 1. Praxisteil: Knacken von Cäsar-Codes
   b) Vigenère-Chiffre
      → 2. Praxisteil: Knacken von Vigenère-Codes
   c) Playfair

UNIVERSITÄT BAYREUTH

Überblick

1. **Klassische Verfahren:**
   a) Cäsar-Chiffre
      → 1. Praxisteil: Knacken von Cäsar-Codes
   b) Vigenère-Chiffre
      → 2. Praxisteil: Knacken von Vigenère-Codes
   c) Playfair

2. **Moderne Kryptographie – Sicherheit im Internet**
      → 3. Praxisteil: Das Rucksack-Problem

UNIVERSITÄT BAYREUTH

Die Cäsar-Chiffre

Beispiel (Geheimes Treffen):

`treffpunkt um zwei vor der schule`

wird verschlüsselt zu

`usfgggqvolu vn axfj wps efs tdivmf`

UNIVERSITÄT BAYREUTH

Die Cäsar-Chiffre

Beispiel (Geheimes Treffen):

`treffpunkt um zwei vor der schule`

wird verschlüsselt zu

`usfggqvolu vn axfj wps efs tdivmf`

- Verschiebung um einen Buchstaben
- „Schlüssel D“ bedeutet z.B. A wird zu D (alle Buchstaben werden um 3 Buchstaben verschoben).
- Im Beispiel haben wir Schlüssel B benutzt.
- 25 Möglichkeiten

UNIVERSITÄT BAYREUTH

Knacken von Cäsar-Codes

Beispiel:

```
xkdofcc rj bic slk tbpqbk
```

UNIVERSITÄT BAYREUTH

Knacken von Cäsar-Codes

Beispiel:

`xkdofcc rj bic slk tbpqbk`

Anfang für verschiedene Schlüssel:

`ylepgdd (+1)`

UNIVERSITÄT BAYREUTH

Knacken von Cäsar-Codes

Beispiel:

`xkdofcc rj bic slk tbpqbk`

Anfang für verschiedene Schlüssel:

`ylepgdd (+1)`

`zmfqhee (+2)`

UNIVERSITÄT BAYREUTH

Knacken von Cäsar-Codes

Beispiel:

```
xkdofcc rj bic slk tbpqbk
```

Anfang für verschiedene Schlüssel:

```
ylepgdd (+1)
zmfqhee (+2)
angriff (+3)
```

UNIVERSITÄT BAYREUTH

Knacken von Cäsar-Codes

Beispiel:

`xkdofcc rj bic slk tbpqbk`

Anfang für verschiedene Schlüssel:

`ylepgdd (+1)`

`zmfqhee (+2)`

`angriff (+3)`

→ Verschiebung um +3 sinnvoll:

`angriff um elf von westen`

UNIVERSITÄT BAYREUTH

Vigenère-Chiffre

Verschlüsselung eines geheimen Treffpunkts:

```
treffen um zwei vor der schule
```

UNIVERSITÄT BAYREUTH

Vigenère-Chiffre

Verschlüsselung eines geheimen Treffpunkts:

`treffen um zwei vor der schule`

Idee:

n-fache Anwendung von Caesar, n>1

UNIVERSITÄT BAYREUTH

Vigenère-Chiffre

Verschlüsselung eines geheimen Treffpunkts:

`treffen um zwei vor der schule`

Idee:

n-fache Anwendung von Caesar, n>1

Hier stark vereinfacht: n=2

`treffen um zwei vor der schule`

UNIVERSITÄT BAYREUTH

Vigenère-Chiffre

Verschlüsselung eines geheimen Treffpunkts:

`treffen um zwei vor der schule`

Idee:

n-fache Anwendung von Caesar, n>1

Hier stark vereinfacht: n=2

`treffen um zwei vor der schule`

Verschiebung um 3 bzw. 5 (Schlüssel „DF“)

`-> wwhkijq zp ezjl arw gju xfmxqh`

UNIVERSITÄT BAYREUTH

Knacken von Vigenère: Häufigkeitsanalyse

Annahme:

Wir wissen, dass n=2 ist (im Allgemeinen muss n erst bestimmt werden).

UNIVERSITÄT BAYREUTH

Knacken von Vigenère: Häufigkeitsanalyse

Annahme:

Wir wissen, dass n=2 ist (im Allgemeinen muss n erst bestimmt werden).

Idee der Häufigkeitsanalyse (vereinfacht):

Der Buchstabe e tritt in der deutschen Sprache viel häufiger auf als alle anderen.

UNIVERSITÄT BAYREUTH

Knacken von Vigenère: Häufigkeitsanalyse

Annahme:

Wir wissen, dass n=2 ist (im Allgemeinen muss n erst bestimmt werden).

Idee der Häufigkeitsanalyse (vereinfacht):

Der Buchstabe e tritt in der deutschen Sprache viel häufiger auf als alle anderen.

→ Schlüssel lassen sich so erraten

UNIVERSITÄT BAYREUTH

Knacken von Vigenère: Häufigkeitsanalyse

Beispiel: `ishcifvfrnmuwdlmehwbloi`

`is hs if vf rn mu wd lm eh wb lo i`

UNIVERSITÄT BAYREUTH

Knacken von Vigenère: Häufigkeitsanalyse

Beispiel: `ishcifvfrnmuwdlmehwbloi`

`is hs if vf rn mu wd lm eh wb lo i`

Häufigkeitsanalyse: Buchstaben zählen

Weiße Buchstaben: Am häufigsten: i

Gelbe Buchstaben: Am häufigsten: f

UNIVERSITÄT BAYREUTH

Knacken von Vigenère: Häufigkeitsanalyse

Beispiel: `ishcifvfrnmuwdlmehwbloi`

`is hs if vf rn mu wd lm eh wb lo i`

Häufigkeitsanalyse: Buchstaben zählen

Weiße Buchstaben: Am häufigsten: i

Gelbe Buchstaben: Am häufigsten: f

Teste i=e und f=e, also Schlüssel EB:

UNIVERSITÄT BAYREUTH

Knacken von Vigenère: Häufigkeitsanalyse

Beispiel: `ishcifvfrnmuwdlmehwbloi`

`is hs if vf rn mu wd lm eh wb lo i`

Häufigkeitsanalyse: Buchstaben zählen

Weiße Buchstaben: Am häufigsten: i

Gelbe Buchstaben: Am häufigsten: f

Teste i=e und f=e, also Schlüssel EB:

`er db ee re nm it sc hl ag sa hn e`

`Erdbeeren mit Schlagsahne`

UNIVERSITÄT BAYREUTH

Playfair

Das Playfair-Quadrat

E	N	I	G	M
A				

UNIVERSITÄT BAYREUTH

Playfair

Das Playfair-Quadrat

E	N	I	G	M
A				

→

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

UNIVERSITÄT BAYREUTH

Playfair: Verschlüsselung

Playfair-Quadrat:

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

Verschlüsselung von Buchstabenpaaren:

Playfair: Verschlüsselung

Playfair-Quadrat:

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

Verschlüsselung von Buchstabenpaaren:

- Gleiche Zeile: Je ein Buchstabe weiter links (ng)

Playfair: Verschlüsselung

Playfair-Quadrat:

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

Verschlüsselung von Buchstabenpaaren:

- Gleiche Zeile: Je ein Buchstabe weiter links (ng->ei)

UNIVERSITÄT BAYREUTH

Playfair: Verschlüsselung

Playfair-Quadrat:

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

Verschlüsselung von Buchstabenpaaren:

- Gleiche Zeile: Je ein Buchstabe weiter links (ng->ei)
- Gleiche Spalte: Je ein Buchstabe weiter oben (yd)

UNIVERSITÄT BAYREUTH

Playfair: Verschlüsselung

Playfair-Quadrat:

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

Verschlüsselung von Buchstabenpaaren:

- Gleiche Zeile: Je ein Buchstabe weiter links (ng->ei)
- Gleiche Spalte: Je ein Buchstabe weiter oben (yd->tg)

UNIVERSITÄT BAYREUTH

Playfair: Verschlüsselung

Playfair-Quadrat:

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

Verschlüsselung von Buchstabenpaaren:

- Gleiche Zeile: Je ein Buchstabe weiter links (ng->ei)
- Gleiche Spalte: Je ein Buchstabe weiter oben (yd->tg)
- Sonst: In gleicher Zeile den Buchstaben der Spalte des anderen verwenden (la)

Playfair: Verschlüsselung

Playfair-Quadrat:

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

Verschlüsselung von Buchstabenpaaren:

- Gleiche Zeile: Je ein Buchstabe weiter links (ng->ei)
- Gleiche Spalte: Je ein Buchstabe weiter oben (yd->tg)
- Sonst: In gleicher Zeile den Buchstaben der Spalte des anderen verwenden (la->hc)

Playfair: Beispiel

Beispiel:

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

Universitaet Bayreuth

UNIVERSITÄT BAYREUTH

Playfair: Beispiel

Beispiel:

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

Universitaet Bayreuth → un iv er si ta et ba yr eu th

UNIVERSITÄT BAYREUTH

Playfair: Beispiel

Beispiel:

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

Universitaet Bayreuth → un iv er si ta et ba yr eu th

Playfair: Beispiel

Beispiel:

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

Universitaet Bayreuth → un iv er si ta et ba yr eu th

→ rm

UNIVERSITÄT BAYREUTH

Playfair: Beispiel

Beispiel:

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

Universitaet Bayreuth → un iv er si ta et ba yr eu th

→ rm ex

UNIVERSITÄT BAYREUTH

Playfair: Beispiel

Beispiel:

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

Universitaet Bayreuth → un iv er si ta et ba yr eu th

→ rm ex nq

UNIVERSITÄT BAYREUTH

Playfair: Beispiel

Beispiel:

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

Universitaet Bayreuth → un iv er si ta et ba yr eu th

→ rm ex nq lx

UNIVERSITÄT BAYREUTH

Playfair: Beispiel

Beispiel:

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

Universitaet Bayreuth → un iv er si ta et ba yr eu th

→ rm ex nq lx qd gq af wt mq qo

UNIVERSITÄT BAYREUTH

Playfair: Entschlüsselung

Beispiel:

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

Entschlüsseln: Andere Richtung bei gleicher Zeile/Spalte, ansonsten gleiche Methode!

rm ex nq lx qd gq af wt mq qo

UNIVERSITÄT BAYREUTH

Playfair: Entschlüsselung

Beispiel:

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

Entschlüsseln: Andere Richtung bei gleicher Zeile/Spalte, ansonsten gleiche Methode!

rm ex nq lx qd gq af wt mq qo

→ **un**

UNIVERSITÄT BAYREUTH

Playfair: Entschlüsselung

Beispiel:

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

Entschlüsseln: Andere Richtung bei gleicher Zeile/Spalte, ansonsten gleiche Methode!

rm ex nq lx qd gq af wt mq qo

→ **un iv er si**

Playfair: Entschlüsselung

Beispiel:

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

Entschlüsseln: Andere Richtung bei gleicher Zeile/Spalte, ansonsten gleiche Methode!

rm ex nq lx qd gq af wt mq qo

→ **un iv er si ta et ba yr eu th**