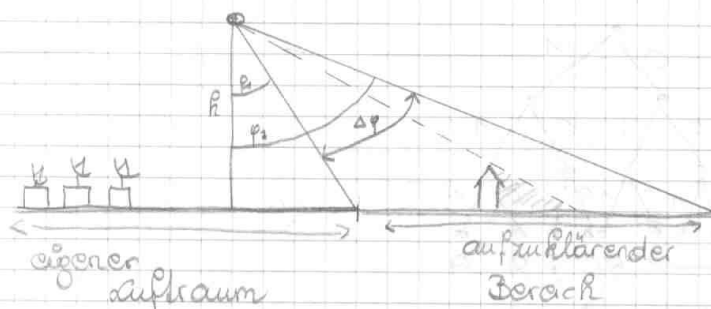


Dienstag 6.11.07

Cryptographie

Anwendungen:

- Botschaften
- Militärische Projekte
 - SLAR = Side looking airborne Radar



- Banken
- Telebanking

Cryptographie = Verschlüsseln von Daten und Texten

Verschlüsselungsmethode

- Ersetzungsmethode
- Verschiebungsmethode

Ersetzungsmethode

Vereinbarung:

unverschlüsselter Text $\rightarrow$ Kleinbuchstaben
plain Text

verschlüsselter Text $\rightarrow$ Großbuchstaben
cipher Text

Methode: 1 Zeichen $\rightarrow$ 1 Zeichen
plain Text cipher Text

z.B. a b c ... x y z
Q W E ... B N M

→ $26! \approx 4 \cdot 10^{26}$... Möglichkeiten der
Anordnung
durch $p(x)$ leicht lösbar!
Verschiebungsmethode

deutsche alphabet 26x verschieben → Matrix

A	B	→	C	D	E	F	...	X	Y	Z
B			C	D	E	F	G	...	Y	Z
Z			A	B	C	D	E	...	W	X

mit diesen Verschiebungen und einem
~~Schlüssel~~ Schlüsselwort haben Agenten
im 2. Weltkrieg kommuniziert

Keyword: MIRACULIX

MIRACULIXMIRACUL...

plain text: langweiliger prof
1. MIRACULIX

→ M N O P Q R S T U V W X Y Z A B C D E F
a b c d e f g h i j k L m n o p q r s t
L → X

2. MIRACULIX

→ I J K L M N O P Q R S T ...
a b c d e f g ...

a → I

8. MIRACULIX

→ J K L M N O P Q R S T U ...
a b c d e f g h i j k l m ...

$L \rightarrow T$

einmal: $L \rightarrow x$ $\left. \begin{array}{l} p(x) \\ L \rightarrow T \end{array} \right\}$ fällt weg

ziemlich sicher:

je länger das Codewort um so besser

Keyword ASTERIX

Bedingung: jeder Buchstabe des Keyword nur einmal enthalten!

A = 1 E = 2 I = 3 R = 4

S = 5

T = 6

X = 7

Nummerierung bezogen auf den Anfang des Alphabets

↓ A	↓ S	↓ T	↓ E	↓ R	↓ I	↓ X
1	5	6	2	4	3	7
l	a	n	g	w	e	i
l	i	g	e	r	p	r
o	p	e	s	s	o	r

→ H o g e s e p o w r s a i f n g e i r r

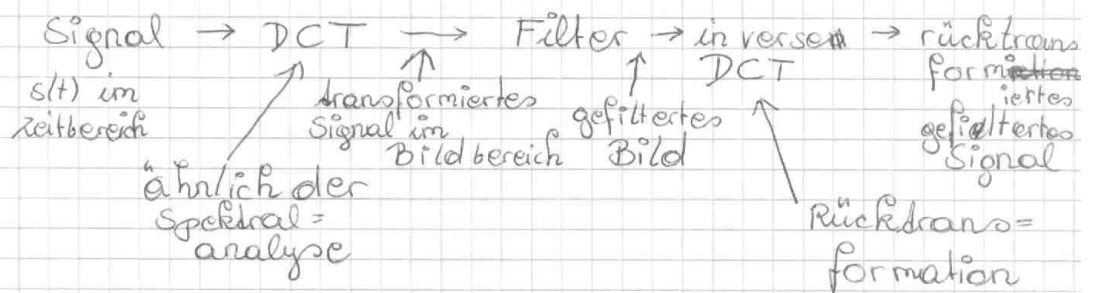
Versuch den Schlüssel zu knacken:

Abzählen $\rightarrow$ auf n -Zeilen
probieren rückzuschließen

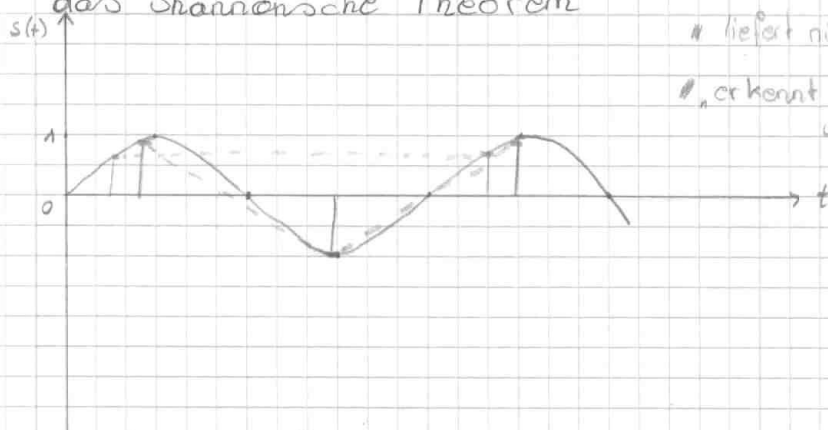
DES, RSA $\Rightarrow$ im Buch!

- Elektronisches Geld
z.B. Telebanking

Diskrete Cosinus-Transformation
(Aufbau des DCT-Filter)



das Shannonsche Theorem



ursprüngliches Signal $s(t)$ Frequenz der Obergrenze f_{OG}

$f_{\text{Abtast}} > 2 f_{\text{OG}}$

Frequenz der Abtastung
muss min. $2 f_{\text{OG}}$ sein