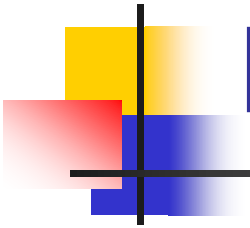
Kryptographie und Datensicherheit

Universität Potsdam
Institut für Informatik
Almahameed Ayman
almahame@uni-potsdam.de

Inhalt des Vortrags

- Einführung
- Grundlagen der Wahrscheinlichkeitstheorie
- Begriff der perfekten Sicherheit
- Entropie und Redundanz
- Produkte von Kryptosystemen

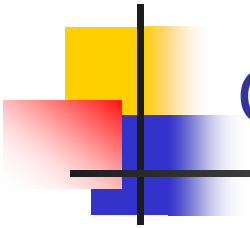


Einführung

- Claude Elwood Shannon (1916 – 2001)
- Mathematiker, Mitarbeiter der Forschungsabteilung von AT&T, Bell Labs, in NJ, Princeton

Informationstheorie

- Die Informationstheorie ist von Shannon begründet
- Jahr 1949
- Die Informationstheorie untersucht :
- Die Darstellung
- Die Speicherung
- Die Übertragung von Informationen



Grundlagen der Wahrscheinlichkeitstheorie

- Definition der Wahrscheinlichkeit
- Einfache Regeln für Wahrscheinlichkeiten
- Satz von Bayes
- Beispiele

Definition der Wahrscheinlichkeit

Klassische Definition der Wahrscheinlichkeit

viele gleichmögliche einander ausschließende Versuchergebnisse , von denen genau eines eintritt

- P(A) = Anzahl der für A günstige Versuchsergebnisse / Anzahl aller mögliche Versuchsergebnisse

Beispiel

- Ein Würfel { 1,2,3,4,5,6}
- Gesucht : die Wahrscheinlichkeit (A)
- (A) ist die Augenzahl durch 2 teilbar
- A = {2,4,3}
- P(A) = 3/6 = ½

Einfache Regeln für Wahrscheinlichkeiten

- Die Summe den Wahrscheinlichkeiten sind 1
- $P(A) + P(\bar{A}) = 1$
- $P(A) \leq P(B)$, falls $A \subseteq$ von B
- $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

Satz von Bayes

- $$P(A \backslash B) = \frac{P(B \backslash A) \cdot P(A)}{P(B)}$$

Beispiel

- Gegeben : 3 Maschinen mit der Gesamtproduktion
- die erste Maschine : 20%
- die zweite Maschine : 30 %
- die dritte Maschine : 50 %
- Ausschluß in der Produktion :
- die erste 5 %
- die zweit : 4 %
- die dritte : 2 %
- Wir berechnen :
- Die Wahrscheinlichkeit der Ausschlußstücks von der ersten Maschine

Beispiel

- Ai ist die Wahrscheinlichkeit für die Maschinen mit i = 1,2,3
- B ist die Wahrscheinlichkeit des Ausschluß
- Gesucht :
- P (A1\ B)

Beispiel

- P (A1\ B) = P (B\ A1) . P(A1) / P (B)
- wir haben :
- P(A1) = 0,2
- P (A2) = 0,3
- P(A3) = 0,5
- auch
- P (B\A1) = 0,05
- P (B\A2) =0,04
- P (B\A3) =0,02

Beispiel

- aber $P_{(B)}$= 0,2*0,05 + 0,3*0,04 + 0,5*0,02 = 0,032
- $P_{(A1\backslash B)}$=(0,05* 0,2)/0,032 = 0,01/0,032 = 0,31.....
- und wir können auch berechnen :
- $P_{(A2\backslash B)}$ =0,38.....
- $P_{(A3\backslash B)}$=0,31.....

Begriff der perfekten Sicherheit

Definition des Kryptosystem

Ein Kryptosystem ist ein Tupel S = (P,C,K , E, D) mit

- P ist Klartext
- C ist Geheimtext
- K ist Keys
- e : ist Chiffrierfunktion
- d : ist Dechiffrierfunktion mit

Beispiel

- P={a,b} mit $P_{(a)}=1/4$,$P_{(b)}=3/4$
- K = {K_1,K_2,K_3} mit $P_{(K1)}=1/2$, $P_{(K2)}=P_{(K3)}$ = ¼
- C ={1,2,3,4}
- $e_{k1(a)}$ =1 , $e_{k1(b)}=2$,$e_{k2(a)}=2$,$e_{k2(B)}=3$, $e_{k3(a)}=3$,$e_{k3(b)}=4$

Beispiel

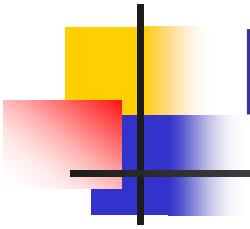
- Diese Kryptosystem wird durch Matrix gegeben

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Beispiel

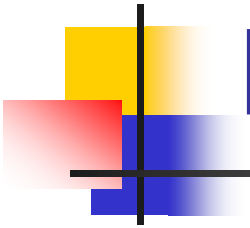
- Satz
- Die Wahrscheinlichkeit , mit der ein Geheimtext c auftritt, wird bistimmt durch:
- $P_{(c)} = \sum P_{(K)} \cdot P_{(p)}$

p= dk(c)



Beispiel

- $P_c(1) = P(k_1) \cdot P(a) = ½ \cdot ¼ = 1/8$
- $P_c(2) = P(k_1).P(b)+P(k_2).P(a) =$
- $(1/2*3/4)+(1/4/1/4) = 7/16$
- $P_c(3)=1/4$
- $P_c(4)=3/16$



Beispiel

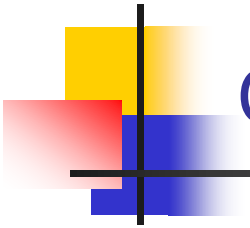
- P(a \ 1) = (P(1 \ a). P(a)) / P(1) = 1
- P(a \ 2) =1/7
- u.s.w

Definition

- Die Krypotosystem ist perfekt , wenn P(x \ y) =P (X)
- x€ P ,y € C
- durch Kenntnis des Geheimtexts

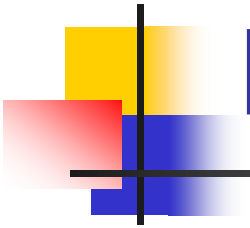
keine Informationen über den Klartext bekannt werden.

- Beispiel : P (a \ 1) ≠ P(a)



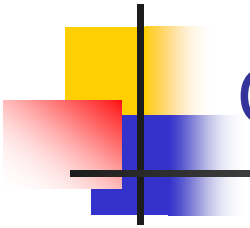
One-Time Pad

- S = (P,C,K , E, D) mit
- P=C=K={0, 1}^n
- e(P, k) = p XOR k
- d(C, k) = c XOR k



Beispiel

- Klartext 11011011
- Schlüssel 00110011
- Geheimtext 11101000
- Schlüssel 00110011
- Klartext 11011011



One-Time Pad

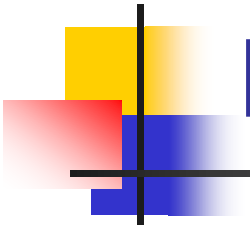
Nachteile

- Der Schlüssel muss genauso lang sein wie der Klartext und dem Empfänger vorliegen
- Jeder Schlüssel wird nur ein einziges Mal verwendet und muss sicher vernichtet werden

Entropie und Redundanz

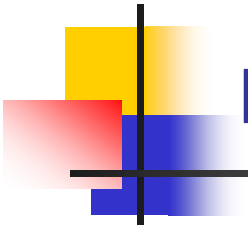
Definition

- Gegeben ein endliche Wahrscheinlichkeitsraum von P mit Elementarereiggnisse in x und Wahrscheinlichkeiten P(x)
- Es gilt $H(P) = -\sum P(x).\log_2 P(x)$
- Heisst Entropie von P
- Wenn $|x| = n$ und $P(x) = 1/n$ dann ist $H(x) = \log_2 n$



Beispiel

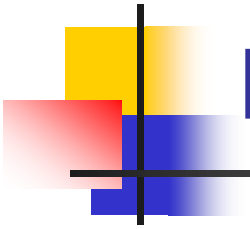
- Gegeben P { a,b} mit P(a) = ½ , P(b)=1/4
- Gesucht H(P)
- $H(P) = -(1/2*\log_2 ½ + 1/4*\log_2 ¼) = 1{,}30\ldots$



Huffmancodierung

Algorithmus Huffman

- suche zwei Knoten *a* und *b* mit minimaler Wahrscheinlichkeit P(a) , P(b) , und addieren
- erzeuge einen neuen Knoten w und verbinde w mit a und b. Markiere die eine Kante mit 0, die andere mit 1. Markiere den Knoten w mit p(a) + p(b)



Beispiel

- Sei X ={a,b,c,d,e} mit P(a)=0.05, P(b)=0.10 , P(c) =0.12 , P(d) =0.13 , P(e) =0.60
- Die Codierungs
- a 000
- b 001
- c 010
- d 011
- e 1

Beispiel

- mittlere Codewortlänge
- $l_{(f)} = \sum_{x \in X} P_{(x)} \cdot |f_{(x)}|$

$$l_{(f)} = 0.05*3 + 0.10*3 + 0.12*3 + 0.13*3 + 0.60*1 = 1.8$$

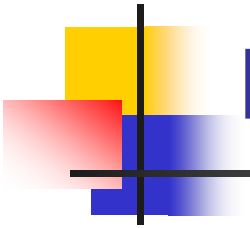
Eigenschaften der Entropie

- $H(X,Y) = \leq H(X) + H(Y)$, mit X , Y sind unabhängige Zufallgrößen
- $H(X|y) = -\sum_{x} P[x|y].\log_2 P[x|y]$
- $H(X|Y) = -\sum_{y}\sum_{x} P[y]P[x|y]\log_2 P[x|y]$
- $H(X,Y) = H(Y) + H(X|Y)$
- $H(X|Y) \leq H(X)$, mit X und Y sind unabhängig.

Redundanz

- Sei L eine natürliche Sprache, die Entropie von L ist definiert $H_L = \lim_{n\neg} H(P\hat{}n) / n$
- Die Redundanz von L ist definiert $R_L = 1 - H_L / \log_2|P|$

Beispiel



- Gegeben : L ist englische Sprache
- $1.0 \leq H_L \leq 1.5$, rund 1.25

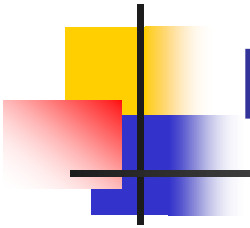
- $R_L = 1 - 1.25 / \log_2 26 = 73{,}4\%$ d.h
- ca. 75% der englische Sprache sind redundant

Definition

- Satz : Ein Krypotosystem (P,C,K,E,D) mit |C| = |P| und sei RLsei die Redundanz der

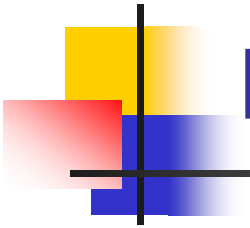
zu Grunde liegenden Sprache mit gegebenen Chiffretext der Länge n, Anzahl falscher Schlüssel Sn ist

$S_n \geq |K| / |P \hat{} n\text{-}R_L|$



Definition

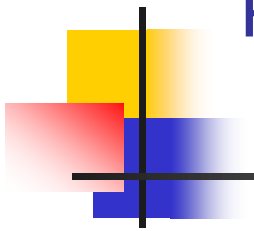
- Die unicity Distance eines Kryptosystems ist definiert : die Anzahl der benötigten Keys, um ein Kryptosystem zu 0 sein
- wenn wir $S_n = 0$ setzen , dann
- $n_0 = \log_2|K| \,/\, R_L \,.\, \log_2 \,.\, |P|$



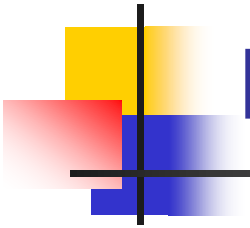
Beispiel

- |P| =26
- |K| = 26 !
- R_L =0.75
- n_0 = 88,4 / (0.75 * 4,7) =25

Produkte von Kryptosystemen



- Verbinden zweier Kryptosysteme zur Erhöhung der Sicherheit
- Diese Kryptosysteme müssen endomorph sein (Geheimtexte =Klartexte)
- Also $S_1 = (P, P, K_1, E_1, D_1)$ und $S_2 = (P, P, K_2, E_2, D_2)$



Eigenschaften

- Wenn M * S =S * M , dh zweier Kryptosysteme sind commute
- Wenn $(S_1 * S_2) * S_3 = S_1 * (S_2 * S_3)$,dh zweier Kryptosysteme sind associative
- Wenn $S^2 = S * S = S$, dh Idempotent:

Literatur

- Douglas Stinson: Cryptography, Theory and Practice, 3. Auflage
- IT Sicherheit , Claudia Eckrad , 3 Auflage
- Brackmann, Roland. http://www.cs.uni-potsdam.de/ti/lehre/05-Kryptographie/slides/shannons_theorie_brackmann.pdf
- Marco Michael, http://www.cs.uni-potsdam.de/ti/lehre/06-Kryptographie/slides/slides-02.pdf
- Prof.Dr.Christoph Kreitz , Kryptographie und Komplexität , Universität Potsdam, Wintersemester 2007/2008