Contents

1	Standard Fragen	2
2	Eigener Verschlüsslungs Algo.	2
3	CBC ECB CTR	3
4	Anhang	3

1 Standard Frage

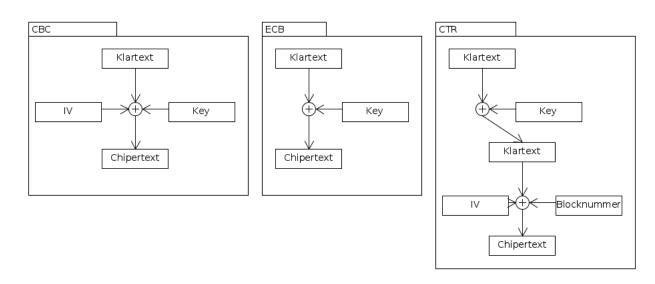
- 1. Wo mit Beschäftigt sich IT-Sicherheit(Definition)? IT-Sicherheit beschäftigt sich mit der Vorbeugung, dem Erkennen und der Reaktion auf Ereignisse, die die Integrität der Daten, die Nutzbarkeit der Systeme und die (digitale) Privatsphäre gefährden.
- 2. Vor welchen drei Gefährdungen müssen Rechner- und Netzwehrkomponenten geschützt werden?
 - Spionage
 - Sabotage
 - Missbrauch
- 3. Nennen Sie die in der Vorlesung genannten drei Schutzziele für Rechnerund Netzkomponenten.
 - Vertraulichkeit
 - Integrität
 - Verfügbarkeit

2 Eigener Verschlüsslungs Algo.

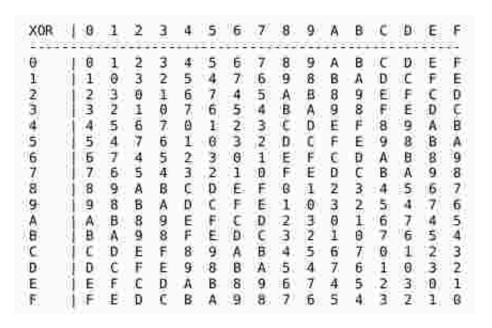
12 Stellige Passwörter werden nach dem Muster abuvcdwxefyz gebildet. Wobei uvwxyz der Passwort Kern &asz6K ist. und ab die ersten beiden Buchstaben der url entsprechen. cd den dritten und vierten Buchstaben welche um ROT+1 verschoben sind. Und schlussendlich ef die letzten beiden Buchstaben welche um ROT-1 verschoben sind. URLs Kürzer als 6 zeichen werden einfach wiederholt.

 $\label{eq:www.heise.de} www.heise.de => heiseh$ abuvcdwxefyz $\label{eq:he&ajtszdg6K} he\&ajtszdg6K$

3 CBC ECB CTR



4 Anhang



ASCI Tabelle

1. Num Lock einschalten

2. ALT + ASCI Zahl Beispiel: ALT+64 = @

001	ASCI	Zeichen	ASCI	Zeichen	ASCI	Zeichen	ASCI	Zeichen	ASCI	Zeichen	ASCI	Zeichen
	000	(Null)	046	-	92	١	138	è	184	©	230	μ
003 ▼ 049 1 95	001	☺	047	/	93]	139	Ϊ	185	네	231	þ
004	002	•	048	0	94	٨	140	î	186		232	Þ
005 ♣ 051 3 97 a 143 å 189 ¢ 235 Ù 006 ♣ 052 4 98 b 144 È 190 ¥ 236 ý 007 • 053 5 99 c 145 æ 191 ¬ 237 Ý 008 □ 054 6 100 d 146 Æ 192 □ 238 □ 009 ○ 055 7 101 e 147 ô 193 □ 239 ○ 010 ■ 056 8 102 f 148 ô 194 ¬ 240 ¬ 011 ♂ 056 8 102 f 148 ô 194 ¬ 240 ¬ 011 ♂ 057 9 103 g 149 ô 195 □ 241 ± 012 ♀ 058 □ 104 h 150 û 196 — 242 □ 013 Ј 059 ⋮ 105 i 151 ù 197 → 243 ¾ 014 Ј 060 < 106 i 152 ý 188 à 244 ¶ 015 ⋈ 061 = 107 k 153 Ö 199 Ä 245 § 016 ▶ 062 > 108 □ 155 ѝ 201 □ 246 → 017 ◀ 063 ? 109 m 155 ѝ 201 □ 247 □ 018 ♀ 068 Ø 110 n 156 Æ 202 □ 248 ○ 019 № 065 A 111 0 157 Ø 203 □ 249 □ 020 ¶ 066 C 113 q 159 f 205 □ 251 □ 020 ¶ 066 B 112 p 158 × 204 □ 250 □ 021 § 067 C 113 q 159 f 205 □ 251 □ 022 — 068 D 114 r 160 à 266 □ 252 □ 023 ♀ 069 E 115 S 161 i 209 Ð 255 ((leer)) 025 □ 070 F 116 t 162 ô 288 ô 254 ■ 026 □ 071 G 117 U 183 Ú 209 Ð 255 ((leer)) 031 ▼ 077 M 123 ⟨ 169 № 155 № 211 Ē 032 □ 070 G 119 W 165 № 211 Ē 033 □ 070 O 125 ⟩ 171 ½ 271 □ 034 □ 080 P 126 ~ 172 ¼ 218 □ 035 # 081 Q 127 ∩ 173 i 219 □ 036 № 8 W 132 & 166 □ 212 È 037 № 83 S 129 Û 175 № 221 □ 038 № 8 W 1 130 ♠ 177 □ 226 Ø 039 № 85 U 131 à 177 □ 225 Ø 040 (86 V 132 à 136 È 182 Å 228 Ø	003	Y	049	1	95		141		187	a ה	233	
006	004	♦	050	2	96	`	142	Ä	188	긔	234	Û
007	005	*	051	3	97	а	143	å	189	¢	235	Ù
008	006	^	052	4	98	b	144	É	190	¥	236	J
000	007	•	053	5	99	С	145	æ	191	٦	237	Ý
010	800	•	054	6	100	d	146	Æ	192	L	238	_
011	009	0	055	7	101		147	ô	193	上	239	,
012	010		056	8	102	f	148	Ö	194	Т	240	-
013	011	8	057	9	103	g	149	Ò	195	-	241	±
014	012	7	058		104	h	150	û	196	_	242	
015	013	2	059	,	105	i	151	ù	197	+	243	3/4
108	014	,	060	<	106	j	152		198		244	¶
017	015	☆	061	=	107	k	153	Ö	199	Ã	245	§
018	016		062	>	108	1	154	Ü	200	L	246	÷
110	017	◀	063	?	109	m	155	Ø	201	F	247	,
020 ¶ 066 B 112 p 158 × 204	018	1	064	@	110	n	156	£	202		248	0
020 ¶ 066 B 112 p 158 × 204	019	!!	065	Α	111	0	157	Ø	203	╦	249	
S	020	¶	066	В	112	р	158	×	204	- 11	250	
Description Description	021	§	067	С	113		159	f	205	=	251	1
023 ↓ 069 E 115 S 161 Í 207 □ 253 ² 024 ↑ 070 F 116 t 162 Ó 208 Õ 254 ■ 025 ↓ 071 G 117 u 163 ú 209 Đ 255 (leer) 026 → 072 H 118 V 164 ñ 210 È 027 ← 073 I 119 W 165 Ñ 211 È 028 L 074 J 120 x 166 a 212 È 029 → 075 K 121 y 167 o 213 I 030 ▲ 076 L 122 z 168 ¿ 214 Í 031 ▼ 077 M 123 { 169 ® 215 Î 032 (Leerstelle) 078 N 124 170 <td>022</td> <td>_</td> <td>068</td> <td>D</td> <td>114</td> <td></td> <td>160</td> <td>á</td> <td>206</td> <td>#</td> <td>252</td> <td>3</td>	022	_	068	D	114		160	á	206	#	252	3
025 ↓ 071 G 117 U 163 Û 209 Đ 255 (leer) 026 → 072 H 118 V 164 Ñ 210 Ê 027 ← 073 I 119 W 165 Ñ 211 Ë 028	023	1	069	Е	115	s	161	ĺ	207	1 **	253	2
026 → 072 H 118 V 164 ñ 210 Ê 027 ← 073 I 119 W 165 Ñ 211 Ë 028 L 074 J 120 X 166 a 212 È 029 ↔ 075 K 121 Y 167 o 213 I 030 ▲ 076 L 122 z 168 ¿ 214 Í 031 ▼ 077 M 123 { 169 ® 215 ĵ 032 (Leerstelle) 078 N 124 170 ¬ 216 ï 033 ! 079 O 125 } 171 ½ 217 J 034 " 080 P 126 ~ 172 ¼ 218 _ 035 # 081 Q 127 △ 173 j 219 _ 036 \$	024	<u> </u>	070	F	116	t	162	Ó	208	ð	254	
027 ← 073 I 119 W 165 Ñ 211 Ë 028	025	\downarrow	071	G	117	u	163	ú	209		255	(leer)
028 □ 074 J 120 x 166 a 212 E 029 ↔ 075 K 121 y 167 o 213 I 030 ▲ 076 L 122 z 168 ¿ 214 Í 031 ▼ 077 M 123 { 169 ® 215 Î 032 (Leerstelle) 078 N 124 170 ¬ 216 Ï 033 ! 079 O 125 } 171 ½ 217 □ 034 " 080 P 126 ~ 172 ¼ 218 □ 035 # 081 Q 127 □ 173 i 219 □ 036 \$ 82 R 128 Ç 174 « 220 □ 037 % 83 S 129 Ü 175 » 221 □ 038	026	\rightarrow	072	Н	118	V	164	ñ	210			
029	027	←	073		119	W	165	Ñ	211	Ë		
029	028	L	074	J	120	Х	166	а	212	È		
031 ▼ 077 M 123 { 169 ® 215 Î 032 (Leerstelle) 078 N 124 170 ¬ 216 Ï 033 ! 079 O 125 } 171 ½ 217 034 " 080 P 126 ~ 172 ¼ 218 035 # 081 Q 127 □ 173 ¡ 219 □ 1036 \$ 82 R 128 Ç 174 « 220 □ 1037 % 83 S 129 Ü 175 » 221 ┆ 1038 & 84 T 130 é 176 039 85 U 131 â 177 □ 223 □ 1040 (86 V 132 ä 178 □ 224 Ó 178 □ 225 ß 1042 * 88 X 134 å 180 ¬ 226 Ô 1044 , 90 Z 136 ê 182 Â 228 Õ	029	\leftrightarrow	075	K	121	у	167	0	213	I		
031 ▼ 077 M 123 { 169 ® 215 Î 032 (Leerstelle) 078 N 124 170 ¬ 216 Ï 033 ! 079 O 125 } 171 ½ 217 034 " 080 P 126 ~ 172 ¼ 218 035 # 081 Q 127 □ 173 ¡ 219 □ 1036 \$ 82 R 128 Ç 174 « 220 □ 1037 % 83 S 129 Ü 175 » 221 ┆ 1038 & 84 T 130 é 176 039 85 U 131 â 177 □ 223 □ 1040 (86 V 132 ä 178 □ 224 Ó 178 □ 225 ß 1042 * 88 X 134 å 180 ¬ 226 Ô 1044 , 90 Z 136 ê 182 Â 228 Õ	030	A	076	L	122	Z	168	i	214	ĺ		
033 ! 079 O 125 } 171 ½ 217 J 034 " 080 P 126 ~ 172 ¼ 218 F 035 # 081 Q 127 △ 173 j 219 □ 036 \$ 82 R 128 Ç 174 « 220 □ 037 % 83 S 129 Ü 175 » 221 □ 038 & 84 T 130 é 176 222 □ 039 85 U 131 â 177 223 □ 040 (86 V 132 ä 178 224 Ó 041) 87 W 133 à 179 225 ß 042 * 88 X 134 å 180 - 226 Ô 043 + 89 Y 135 Ç 181	031	▼	077	М	123	{	169		215	ĵ		
034 " 080 P 126 ~ 172 ½ 218 □ 035 # 081 Q 127 △ 173 ¡ 219 □ 036 \$ 82 R 128 Ç 174 « 220 □ 037 % 83 S 129 □ 175 » 221 ¹ 038 & 84 T 130 é 176 222 ¹ 039 85 U 131 â 177 223 □ 040 (86 V 132 ä 178 224 Ó 041) 87 W 133 à 179 225 ß 042 * 88 X 134 å 180 - 226 Ô 043 + 89 Y 135 Ç 181 Å 227 Ò 044 , 90 Z 136 ê 182	032	(Leerstelle)	078	N	124		170	٦	216	Ϊ		
034	033	!	079	0	125	}	171	1/2	217			
035 # 081 Q 127 △ 173 ¡ 219 □ 036 \$ 82 R 128 Ç 174 « 220 □ 037 % 83 S 129 Ü 175 » 221 ⋮ 038 & 84 T 130 é 176 222 ⋮ 039 85 U 131 â 177 223 □ 040 (86 V 132 ä 178 224 Ó 041) 87 W 133 à 179 225 ß 042 * 88 X 134 å 180 - 226 Ô 043 + 89 Y 135 Ç 181 Á 227 Ò 044 , 90 Z 136 ê 182 Â 228 Õ	034	"	080	Р	126	~	172	1/4	218	Г		
036 \$ 82 R 128 Ç 174 « 220 ■ 037 % 83 S 129 ü 175 » 221 ļ 038 & 84 T 130 é 176 222 j 039 85 U 131 â 177 223 □ 040 (86 V 132 ä 178 224 Ó 041) 87 W 133 à 179 225 ß 042 * 88 X 134 å 180 - 226 Ô 043 + 89 Y 135 Ç 181 Á 227 Ò 044 , 90 Z 136 ê 182 Â 228 õ	035	#	081	Q	127	Δ		i	1		1	
037 % 83 S 129 ü 175 » 221 I 038 & 84 T 130 é 176 222 I 039 85 U 131 â 177 223 □ 040 (86 V 132 ä 178 224 Ó 041) 87 W 133 à 179 225 ß 042 * 88 X 134 å 180 - 226 Ô 043 + 89 Y 135 Ç 181 Á 227 Ò 044 , 90 Z 136 ê 182 Â 228 Õ	036		82		128	Ç	174	«	220		1	
038 & 84 T 130 é 176 222 Ì 039 85 U 131 â 177 223 □ 040 (86 V 132 ä 178 224 Ó 041) 87 W 133 à 179 225 ß 042 * 88 X 134 å 180 - 226 Ô 043 + 89 Y 135 Ç 181 Á 227 Ò 044 , 90 Z 136 ê 182 Â 228 õ	037		83					»		I I	1	
039 85 U 131 â 177 223 □ 040 (86 V 132 ä 178 224 Ó 041) 87 W 133 à 179 225 ß 042 * 88 X 134 å 180 - 226 Ô 043 + 89 Y 135 Ç 181 Á 227 Ò 044 , 90 Z 136 ê 182 Â 228 õ	038		84		130		176		222	Ì	1	
040 (86 V 132 ä 178 224 Ó 041) 87 W 133 à 179 225 ß 042 * 88 X 134 å 180 - 226 Ô 043 + 89 Y 135 ç 181 Á 227 Ò 044 , 90 Z 136 ê 182 Â 228 Õ	039		85		1		1	******			1	
041) 87 W 133 à 179 225 ß 042 * 88 X 134 å 180 - 226 Ô 043 + 89 Y 135 Ç 181 Á 227 Ò 044 , 90 Z 136 ê 182 Â 228 Õ	040	(Ó	1	
042 * 88 X 134 å 180 - 226 Ô 043 + 89 Y 135 Ç 181 Á 227 Ò 044 , 90 Z 136 ê 182 Â 228 Õ	041)		W				IT			1	
043 + 89 Y 135 Ç 181 Å 227 Ò 044 , 90 Z 136 ê 182 Â 228 Õ	042	*			1		1	H			1	
044 , 90 Z 136 Ê 182 Â 228 Õ	043	+			1		1	Á			1	
	044	,			•						1	
	045	"_"		Γ							1	

1 IP Tables

1.1 Initialisieren

```
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

1.2 NAT (Port Forwarding)

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 443 -j DNAT --to 192.168.0.x:443

-t = Tabelle
    -A = Füge Regel zu ausgewählter Kette hinzu
    PREROUTING: Bearbeiten der Pakete sobald sie reinkommen
    POSTROUTING: Pakete erst bearbeiten, sobald sie rausgehen
    -o = out-interface
    -i = in-interface
    -p = Protkoll
    --dport = Destination Port
    --sport = Source Port
    eth0 = In diesem Fall Interface zum Internet
    eth1 = In diesem Fall Interface ins Interne Netz
    -j = Auszuführende Regel
```

1.3 Beispiel Forwarding Regel

```
iptables -A FORWARD -p tcp -i eth0 -d 192.168.101.x --dport 443 -j ACCEPT
iptables -A FORWARD -p tcp -o eth0 -s 192.168.101.x --sport 443 -j ACCEPT
    -d = destination IP
    -s = source IP
```

1.4 Beispiel Nur hergestellte Verbindung

```
iptables -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
-m = match
--state = der zu vergleichende Status
```

1.5 Beispiel DHCP-Server

2 Funktionen & Bedenklichkeiten

Bedenklich	Attacke	Verbesserung					
char *gets(char *str);	Buffer	char *fgets(char *str, int num, FILE *stream);					
gets(song)	Overflow	fgets(song, sizeof(song), stdin)					
<pre>int sprintf(char *str, const char *fomat,);</pre>		int snprintf(char *s, size_t n, const char * format,);					
<pre>int sprintf(command, "get %s.mp3", song);</pre>	Overflow	<pre>int snprintf(command, sozeof(command), "get%s.mp3", song); command[sizeof(command)-1]='\0';</pre>					
size_t strlen(const char *s);	Buffer	size_t strnlen(const char *s, size_t maxlen);					
len = strlen(str);	Overflow	len = strnlen_s(str, sizeof str);					
char * strcpy (char * destination, const char * source);	Buffer Overflow	size_t strlcpy(char *destination, const char *source, size_t size); ODER char * strncpy(char *destination, const char *source, size_t size);					
strcpy (str2,str1);		strncpy (str2, str1, sizeof(str2)); len = strlcpy(str2, str1, sizeof(str2));					
char *strcat(char *destination, const char *source)	Command Injection	size_t strlcat(char *dst, const char *src, size_t size);					
strcat(to, from)		strlcat(to, from, sizeof(to));					
gets(input); [anz. in n= "%s%n\n",buf,&n] printf(input);	Formatstring- Attacke	Herausfiltern der Zeichen. Erkennung → %n (anzahl Zeichen) [input = "%s%n\n",buf,&n]					
filename= mktemp(template); fd = open(filename, O_RDWR);	Race Condition	Zwischen dem erzeugen und dem Öffnen der Datei existiert eine Race Condition, da die Datei in der Zwischenzeit der beiden Aufrufe geändert worden sein könnte					

3 Sonstige Bedenklichkeiten

- Kein Salz
- least privilege
- Rückgabewerte von Funktionen nicht ausgewertet
- · sscanf oder ähnliches
- Signale nicht abgefangen
- Schutz vor Swapping fehlt
- Challenge kein Zufallswert