

Lizenzbestimmungen

- Diese Materialien sind lizenziert für @USERINFONAME@.
- Die Materialien dürfen **ausschließlich** für die Implementation, Verbesserung oder den Betrieb von Sicherheitsmaßnahmen innerhalb der genannten Organisation genutzt werden.
- Hierfür dürfen die Materialien beliebig verändert, ergänzt oder neu gestaltet werden.
- Für alle anderen Einsatzzwecke - insbesondere für die Veröffentlichung der Materialien und deren Einsatz für Kunden des Lizenznehmers - muss im Vorfeld eine schriftliche Genehmigung der 3473 Gurus GbR eingeholt bzw. eine entsprechende Lizenz erworben werden.

Die Seiten dieses Bereiches sollen Ihnen nur einen Eindruck vermitteln, welche Inhalte wir für Sie erarbeitet haben. **Deshalb sind die Inhalte absichtlich „verpixelt“**: mehr und mehr Buchstaben werden auf jeder Seite durch Punkte ersetzt.

Wenn Sie auf alle Inhalte zugreifen möchten, benötigen Sie einen entsprechenden Zugang.

Sie möchten einen Zugang erwerben? Hier finden Sie alle weiteren Informationen!

Dieser Artikel bietet einen kompakten Überblick über die wichtigsten kryptografischen Methoden (symmetrische Verschlüsselung, asymmetrische Verschlüsselung, Hashverfahren und Zertifikate).

Kryptografie

Hier ein kurzer Überblick über die wichtigsten kryptografischen Methoden.

Verfahren

Symm.tri.ch. V.r.chlü...lung

Das Prinzip der symmetrischen Verschlüsselung ist einfach: Daten werden verschlüsselt, indem man einen Algorithmus zusammen mit einem Schlüssel auf die Klartextdaten anwendet. Dabei tritt der Schlüssel, wie der Algorithmus, arbitrar. Die Daten werden wieder entschlüsselt, indem man denselben Algorithmus zusammen mit dem gleichen Schlüssel wie bei der Verschlüsselung auf die verschlüsselten Textdaten anwendet:

$V.r.chl...lt = Alg.r.thm..(Kl.rt.xt, Schl...l)$

$Kl.rt.xt = Alg.r.thm..(V.r.chl...lt, Schl...l)$

Symmetrische Verschlüsselung benutzt zwei verschiedene Schlüssel: einen für die Verschlüsselung und einen für die Entschlüsselung. Die Schlüssel müssen geheim gehalten werden. Beispiele für symmetrische Verschlüsselungsverfahren sind DES, 3DES, AES, IDEA, RC2, RC4, RC5, RC6, ... Etc.

Die symmetrische Verschlüsselung ist sehr einfach zu verstehen, aber sie hat einige Nachteile. Zum Beispiel müssen die Schlüssel geheim gehalten werden, was bei der Übertragung von Daten ein Problem sein kann. Ein weiterer Nachteil ist, dass die Schlüssel für jeden Kommunikationspartner separat übertragen werden müssen.

B.....	V.r.....	N.ch.....
DES, 3DES, AES, IDEA, RC2, RC4, RC5, RC6, ... Etc. L... r b.k... y...r.ch.. V.r.ch... S... h..r.	..hr .ch...; .. k... r.ß. D..... rh..b k.rz.r Z... v.r- bzw.ch..... w.r...	Sch.....ch ..w.....; ..r E.....rh.... Sch..... rh....., b.v.r .r ..h.... D... .. G....b.rch.. k... (H....-E.-Pr.b...)

<...> Die zwei verschiedenen Schlüssel sind für die Verschlüsselung und die Entschlüsselung erforderlich. Ein weiterer Nachteil ist, dass die Schlüssel für jeden Kommunikationspartner separat übertragen werden müssen.

A.y....r..ch. V.r.ch.....

$V.r.ch..... = A...r.h...(K...x., Schl.....1)$

K.r.x. = A.r.h...(V.r.ch.....,Sch.....2)

Sch..... 1 ... Sch..... 2 w.r... z..... rz.... ... v.....r .bh..... S.. w.r... .ch ... Sch.....r b.z.ch... l. .r
Pr.x.. w.r.r .r b.... Sch..... v.r.....ch. (... b.z.ch... .h. ...h..b .ch ... „P.b.c K.y“ ...r „.....ch..
Sch.....“ ... A.y....r.ch. V.r.ch..... „P.b.c-K.y-Kry....“). A.y....r.ch. V.r.hr.. b....r. ... h.... .ch
.ch.h.....ch.. Pr.b.... w.. z.B. .r  Pr...k.rz.r....., ...  K.....ck-Pr.b... .r ... ch.. K.rv...
A.. Gr... .. h.... .. G.....z z. ... y....r.ch.. V.r.hr.,ch.. Pr.z.... S.b..... Tr.....
b....r., ... b....b.. k.b....r w.r... k....., .r w.... .y....r.ch. V.r.ch.....v.r.hr.. b.k....

B.....	V.r....	N.ch....
 RSA,  M.rk.-H.....,  R.b.,  E....., V.r.hr.. ... B....ch.r K.rv.. (ECDSA, C.rv.25519, Br....., C.rv.448)	 Pr.b... .. Sch.....ch.	..hr; .. k..... .r k.... D..... ..rh..b k.rz.r Z... v.r- bzw.ch..... w.r...

A.. z.r V.r..... ..h.... .y....r.ch.. V.r.hr..ch.r, w... ..r ...r .ch... r.ß. Sch..... b.r.b..
w.r.... B... .. A.r.h... RSAk.... b.. 2048b.,r.... w.r. .b 2017 .r E....z v..
Sch..... ...r L.... v. 3096b.. ..h.... B.. .r W.h. .r Sch..... ..z. b.ch...,r R.ch....w...
... .r Sch..... D.. A.w.r.v.rh.... v.. E.b.... Sy.... b.. E....zr Sch..... ..h..b .r.....
..... w.r..., b.v.r E..ch..... ..r.... w.r..

A.. A.r....v. z. RSA ... DSA w.r... ..z... J.hr.. V.r.hr.. ... B....ch.r K.rv.. ...w.ck...,ch ...
k.rz.. Sch..... (256 b.. 512b..)hr h.h. S.ch.rh... b.... ...rch w.... .r.r....r .rb.... ... RSA ... DSA.
D..r ... N.... ECDSA, C.rv.25519, Br..... ... C.rv.448 (G.....ck) b.k..... V.r.hr..rw.... .r.r....r.
... w.r... v.. .k..... Sy.... h.... (j...ch .ch.r)r...z.. W... .hr E....z .. Erw.... .z.... w.r.,
.....r.ch.... Sy.... ... K.....b..... w.r....

H..hv.r..hr..

H..hw.r. = A.r.h...(D.....)

E.. H..h....r.h...r.r.r b....b.. .r.ß. (...r k.....) D.....rch W.r. (... ..
H..hw.r.). Ä...r. .ch ... D..... .ch .r .r...,r. .ch .r H..hw.r. ...r .ch. v.rh.r..hb.r.. W.... M.. H....
v.. H..hv.r..hr.. k...ch.r, ... D..... .v.r....r v.. S....r z.. E.....r .b.r.r.... w.r... Z..... ...
E....z v.. .y....r.ch.. V.r.ch.....v.r.hr.. k... ... Ab....r v.. b....b.. .r.ß. D..... v.r...z.r.. (D.....
S.....r).

B.....	V.r....	N.ch....
 MD4,  MD5 (MD = M..... D.....), SHA-0,  SHA-1,  SHA-2 ... V.r..... SHA-224, SHA-256, SHA-384 ... SHA-512,  SHA-3 (SHA =  S.c.r. H..h A...r..h.), RIPEMD-128, RIPEMD-160, RIPEMD-256, RIPEMD-320 ( RIPEMD = R.c. l....r.y Pr....v.. Ev..... M..... D.....)	-	-

M..... .b. .. b..... S.ch.rh....r.b.... ... v.....z... H..h....r.h...:

- D.. V.r..hr.. SHA-0, MD2, MD4 ... MD5br.ch... SHA-1chw.ch.. D.... V.r..hr..
..ch. ..hr v.rw.... w.r....
- A.. ... Ch... C.....c.... C....r... E... D.z.b.r 2008 h.b.. A.x....r S...r.v, M.rc S.v..., J.c.b A....b..., Arj..
L....r, D.v.. M....r, D.. Ar.. O.v.k ... B.... .. W...r .z...., Schw.ch.. ... MD5-A...r.h... .. H.... ..
C....r. (b....h... ... 200 S.y P.y..... 3)z. w.r... k.....,ch.. CA (...h.) z. .rz..... D.r

R.ch..rv.rb... br..ch...r w.... T...r ... A...ck. ¹⁾ D.. US-CERT h.. J....r 2008r V....r.b....y
N... VU#836068 ..r...h... ..h..., j....ch. V.rw..... v.. MD5 ...z.....

Ak..... .. H..hv.r..hr.. SHA-2, SHA-3 ...RIPEMD-160ch.r.

Z.r....k...

B.....	V.r.....	N.ch.....
 X.509	Z.r....k... .. Pr.b... ..r Sch.....v.r...k.....	... Z.r....k..r .. v.r.r.....w.r... w.. ..r A.....r

Erz..... V.r...z.r.. Z.r....k...

[kry....r....z.r....k..j](#)

E.. Z.r....k.. w.r. rz..., ..r ..rch. Sch..... .. Tr...c....r ...ch.ck. w.r.. D.. Tr...c....r v.....r. ... l.h.b.r
...ch.. Sch..... ..r...z. v.r.ch..... l...r..... w.. z.B.

- N... .. l.h.b.r.
- ... b.. ..r Erz.....z... kry....r....ch.. V.r..hr..
- .r...b..r E.....zzw.ck ... Z.r....k...
- v.. ... b..
- ...

A..ch...ß... ..r. ... Tr...c....rch.. Sch..... .. V.rw.....r.....,b.r b.... .. H..h .rz....
...h..... Sch..... ..y....r..ch v.r.ch..... (r.ch.. S.... .. B...). D.r v.r.ch..... H..h (...
S.....r) w.r. ... Z.r....k.. ..h....

E.. Z.r....k.. w.r. v.r...z.r., ..r ..r E.....r .b.rch.. Sch..... .. V.rw.....r..... .. H..h b.....,
... v.r.ch..... H..h ... Tr...c....r. P.b..c K.ych..... .. Er..b.....r v.r...ch.. S.... ..
Er..b.....ch, Z.r....k.. v.r...z.r.. D..r b..... kry....r....ch.. V.r..hr..r E.....r ...
V.rw.....r..... .. Z.r....k....

Zw..r. A..r.... P....w.r..r bzw. Sch.....

[kry....r....br...-rc-...-w..r..rb.ch-....ck..j](#)

Br...-F.rc.-A..r...

U...r Br...-F.rc.-A..r... (v..ch br... ..rc. „r.h. G.w...“) v.r...h. v..... A...r.b..r..rch..
L..... .. Pr.b..... l. B.r..ch ..r Kry....r.... b..... ..,ch.. Sch..... .y.....ch w.r..., b.. ...
r.ch.... L..... bzw. ..r r.ch.... Sch..... w.r....

V.r..h...w....	V.r.....	N.ch.....
D.. v..... D.rch.r.b..r..rch.. L.....chk.....	D.. L..... w.r. ... S.ch.rh...	D.. V.r..hr.. k... .x.r..r.. 

<....> E.. kry....r..h..ch.. V.r..hr..ch.r, w... k....k..v.r.. A..r.... .. Br...-F.rc. b.k.... Br...-

F.rc.-A.r... (z. B.r... ..r h.h.. A.z.h.ch.r Sch.....)ch. ..rch..hrb.rh.. w.r.. </....>

W.r..rb.ch-A...ck.

W... P...w.r..r ..rr.... w.r... Br...-F.rc.-A.r... ..ch. ..rch..hrb.r ..., k... ..r A.r....r ..chr
W.r..rb.ch-A...ck. ..rch..hr... l. ..r Pr.x.. v.rw..... ..r L....ch.r P...w.r..r, .bch.. P...w.r.
..r....r

V.r..h...w....	V.r.....	N.ch.....
D.. v..... D.rch.r.b..r..r L....ch.r P...w.r..r.	D.r A.r...b.r.ch..b.r.r Z... ..rch..hrb.r.	D.. L.... w.r. ..r, w... ..ch ... P...w.r.r L.... b.....

[search?q=..c....%3A.....r%26.....r&btnl=lucky](#)

Die Seiten dieses Bereiches sollen Ihnen nur einen Eindruck vermitteln, welche Inhalte wir für Sie erarbeitet haben. **Deshalb sind die Inhalte absichtlich „verpixelt“**: mehr und mehr Buchstaben werden auf jeder Seite durch Punkte ersetzt.
Wenn Sie auf alle Inhalte zugreifen möchten, benötigen Sie eine entsprechenden Zugang.

Sie möchten einen Zugang erwerben? Hier finden Sie alle weiteren Informationen!

¹⁾
...h. h...:www.w...../h..hc...h/r....-c./