Repetition

- Wie viel Inhalt können mit einem 1024-Bit Schlüssel übermittelt werden? 1024-Bit.
- Ist das Padding normiert? Ja, in einem RFC
- Grösse Integer? 32- / 64-Bit begrenzt durch Architektur, BigInteger :arrow_right: Spezialbehandlung
- Was ist ein qualifiziertes Zertifikat? Personenzertifikat

Padding

Ist der Text kürzer als der Schlüssel braucht es immer zwingend ein Padding. Ansonsten ist die Sicherheit der Nachricht gefährdet (Füllzeichen).

$x = a + bx + cy$

$x = a + bx + cy$
$a^x * a^y = a^{(x+y)}$
$a^{a_0} * a^{bx} * a^{cy} = a^{a_0+bx+cy} = a^x$
$a_0 = 0 \implies a^{a_0} = 0$
$(xy)^d \equiv x^d * y^d mod n$
$C_1 .... C_2$
$C = \prod C(M_i)^{e^i} mod n \rightarrow M = \prod M_i^{e_i} mod n$

ASN.1 [Abstract Syntax Notation No. 1]

Wichtig: - Basic Encoding Rules (BER) - Distinguished Encoding Rules (DER)

Beschreibungsstruktur

Module

Modulname DEFINITIONS::=BEGIN EXPORTS export liste IMPORTS imports . . . .

www.oid-info.com

Sequence: 30h –> Tag: 0011 0000 Universal: 00 Zusammengesetzt: 1 Sequence: 16

Tag-Value: 30-0B-03-03-00-0F-C1-. . . .

Sequence of Seuquence: 30 - L - 30 - . . . .

Objekt-Identifier

x x 40 + y 1x40 + 2 = 42

Zertifikate

Erzeugung

- Werden oft bei CA erstellt.

Ablauf:
1. Person geht zur RA für die initiale Registrierung (Intermidär).
2. RA bestätigt Identität und leitet den Request der CA weiter.
3. ....
x. PKCS#12-Container geht zurück an die Person (geschützt mit PIN)

Aufbau

ID + Signatur $sS_{p_{CA}}(ID)$ ObjectIdentifier :arrow_right: Signaturtyp + Algorithmus