Asymmetrische Verschlüsselung (RSA+Digitale Signatur)

Arj / Okt-2015

Was sind Vor- und Nachteile der symmetrischen Verschlüsselungsverfahren?

-	Sender und Empfänger müssen gleichen Schlüssel haben
-	Schlüsseltausch benötigt sicheren Kanal
-	Falls sicheren Kanal vorhanden könnte ja die Nachricht selbst darüber übertragen werden
-	Schlüsselmanagement aufwändig : S=n*(n-1)/2 S=Schlüssel, n=Teilnehmer Schlüsselzahl wächst quadratisch !
+	Schlüssel sind „kürzer“ als Nachricht
+	Sicherer Kanal für „kurzen“ Schlüssel ist einfacher zu haben als sicherer Kanal für Nachricht

Asymmetrische Verfahren

Wie in der Einleitung schon angedeutet, wird bei der Public/Privat-Key Kryptografie der Schlüssel auf zwei Teilschlüssel aufgeteilt:

Das heisst, das jeder Teilnehmer folgendes besitzt :

Private-Key : Privater Schlüssel
Dient dem Nachrichten-Empfänger zum Entschlüsseln der Nachricht. Der Private-Key kennt nur der Empfänger bzw. bleibt geheim.

Public-Key : Öffentlicher Schlüssel
Dient zum Verschlüsseln einer Nachricht an die Person, der den Public-Key generiert bzw. veröffentlicht hat. Der Public-Key ist jedermann zugänglich !

Das asymmetrische Verfahren «RSA»

RSA gemäss den Erfindern : Ronald L. **R**ivest, Adi **S**hamir und Leonard **A**dleman (1977)

Die Rechenvorschrift für die **Verschlüsselung** der Nachricht lautet:

$$c = k^e \bmod n$$

Die Rechenvorschrift für die **Entschlüsselung** der Nachricht lautet:

$$k = c^d \bmod n$$

Legende:
c steht für Ciphertext
k steht für Klartext
e und **n** sind der Public Key des Empfängers
d und **n** sind der Secret Key des Empfängers

Die Mathematik ist bei Verschlüsselung und Entschlüsselung dieselbe,
die Koeffizienten dagegen sind verschieden!
Die Funktion $x^y \bmod z$ ist eine sog. Einwegfunktion mit Trapdoor. Damit ist eine Funktion gemeint, die sich ohne eine Zusatzinformation nur schwerlich umkehren lässt.

Das asymmetrische Verfahren «RSA»

Berechnung des Schlüsselpaares (Zahlenbeispiel: Nice-to-know)

Das Verfahren : (Vereinfacht!)

Alice wählt zufällig zwei Primzahlen p ≠ q, die etwa gleich lang sein sollten und berechnet deren Produkt N = p·q. **zB. p=11, q=17, n=11*17=187**

Danach berechnet sie x = (p-1) · (q-1) **x=(11-1)*(17-1)=160**

Alice berechnet x + 1 **x+1=161**

Der Wert e wird ausgewählt, wobei d ein Teiler aus x+1 sein muss.

da 161=7*23

Der zweite Teiler aus x+1 ist d. Es muss gelten: d*e=x+1 .

Unzulässige Werte von d und e (z.B. d=e) werden als unsicher abgelehnt.

sind 7 und 23 geeignete Kandidaten für e und d

Alice erhält :

N , e : public key von Alice

d , N : secret key von Alice

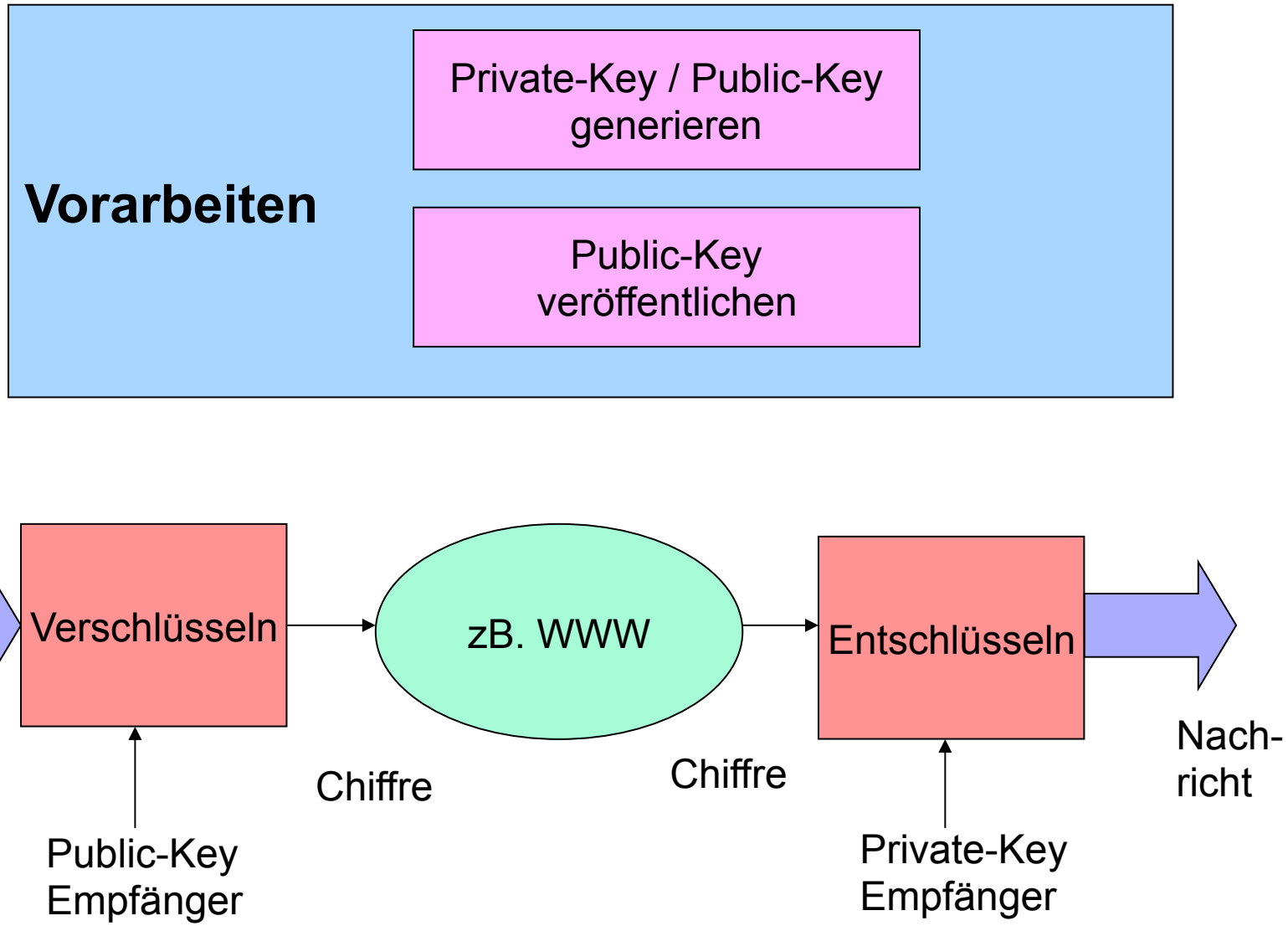
Hybride Verfahren

Bei hybrider Verschlüsselung z.B. bei OpenPGP werden die Vorteile von beiden Verfahren ausgenutzt:

- Asymmetrisches oder Public-Key-Verfahren für Schlüsselmanagement, zB. RSA
- Symmetrisches Verfahren zum Versenden der eigentlichen Nachricht, zB. RC4, DES

	Symmetrisch	Asymmetrisch
Schlüsseltausch	-	+
Rechenzeit	+	-

Das asymmetrische Verfahren «RSA»



Das asymmetrische Verfahren «RSA»

Bemerkung zur Sicherheit der Schlüssel:

Wie in einer vorangegangenen Folie gezeigt, berechnet sich der Schlüssel unter anderem mit diesem Teilschritt:

Alice wählt zufällig zwei Primzahlen $p \neq q$, die etwa gleich lang sein sollten und berechnet deren Produkt $N = p \cdot q$

In einigen Veröffentlichungen wird beschrieben, die Stärke des RSA-Algorithmus basiere auf der Tatsache, dass es schwierig sei, große Primzahlen zu faktorisieren. Dies ist ein Schreibfehler, denn Primzahlen allgemein, groß oder klein, haben nur Zwei Faktoren ;-) Gemeint ist, dass es schwierig ist, große Zahlen zu faktorisieren und der Modulus (p*q) ist eine solche große Zahl.

Digitale Signatur mit «RSA»

- Wer bestellt in meinem E-Shop / Wer schickt mir eine E-Mail ?
- Hat er wirklich das geschrieben was ich lese ?
- Woher kommt das Applet, das gerade auf meinen PC geladen wird ?
- Ist das Update wirklich das “richtige, unmanipulierte” Original ?
- Wohin wird meine Kreditkartennummer übermittelt ?
- Wer gibt einer Wahl gerade seine Wahl-Stimme ab ?
- Stammt der Inhalt von “www.admin.ch” wirklich von unserer Regierung ?

- ***Ausgehend von seinem Grundprinzip ist das Internet nicht sicher:***
- Mitlesen von Daten (Sniffing)
- Vortäuschen falscher Identitäten (Spoofing)
- Angriffe auf die Verfügbarkeit (Denial-of-Service)
- Übertragen von Programmen mit Schadfunktion (Viren, Würmer...)
- Menschliches Fehlverhalten (Preisgabe von geheimen Daten)

- **Authentisierung** Sicherstellung der Identität eines Kommunikationspartners
- **Vertraulichkeit** Zugänglichkeit der Nachricht nur für bestimmten Empfängerkreis
- **Integrität** Schutz vor Verfälschung von Nachrichten bei der Übermittlung
- **Autorisierung** Prüfung der Zugriffsberechtigung auf Ressourcen
- **Verfügbarkeit** Schutz vor Datenverlust, Sicherstellung des laufenden Betriebs
- **Verbindlichkeit** Sicherer Nachweis der Absendung bzw. des Empfangs

Digitale Signatur mit «RSA»

Wesentlicher Ablauf:

- Abbildung des Nachrichteninhaltes auf eine eindeutige Kenngrösse : Hash-Algorithmus
- Identifikation von Kommunikationspartnern durch Digitale Signaturen

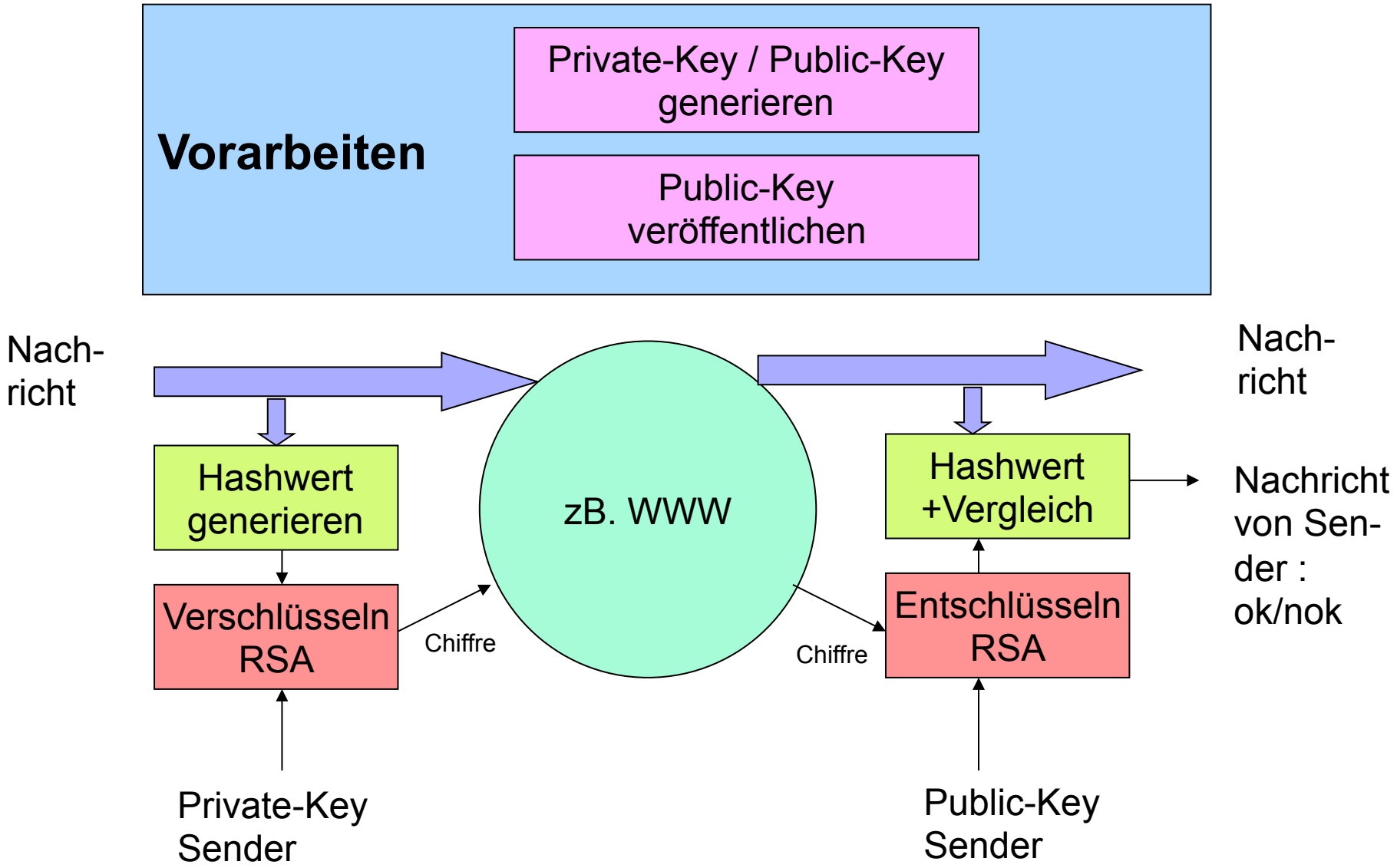
Hash Algorithmus:

- Bilden einen beliebig langen Nachrichtentext auf einen Wert vorgegebener (kurzer) Länge an (Hashwert, “Prüfsumme”)
- Aus Hashwert kann ursprüngliche Nachricht nicht errechnet werden (Irreversibilität)
- Konstruktion von Nachrichten mit gleichem Hashwert muss praktisch unmöglich sein
- Zufällige Übereinstimmung von Hashwerten beliebiger Nachrichten unwahrscheinlich (Kollisionsresistenz, Integrität prüfbar)

Digitale Signatur mit «RSA»

- (Sichere) Identifizierung des Absenders eines Dokumentes
- Sicherheit vor nachträglichen Manipulationen des Dokumentes
- Elektronisch signierte Dokumente sind mit unterschriebenen Papierdokumenten gleich gesetzt
- Ist ein Prüfwert einer Information
- Mit privatem Schlüssel verschlüsselt und zur Information hinzugefügt
- Der Empfänger kann mit Hilfe des öffentlichen Schlüssel des Senders prüfen, ob die Information wirklich vom Absender stammt und nicht verändert wurde
- Die Digitale Signatur hat die Aufgabe einer Unterschrift und eines Siegels.

Digitale Signatur mit «RSA»



Digitale Signatur mit «RSA»

Public Key Infrastruktur:

- ***OpenPGP*** (ein dezentraler Standard)
  Anfangs 90‘ Jahre durch Phil Zimmermann entwickelt :
  Jeder Teilnehmer am Verschlüsselungssystem, der ein gültiges Schlüsselpaar besitzt, kann die Echtheit anderer Schlüssel durch seine Unterschrift bestätigen.

- ***X.509*** (zentral und hierarchisch organisiert)
  der Besitzer hat seine Identität/Glaubwürdigkeit durch ein X-509 Zertifikat von einer **CA** (=**C**ertification **A**uthority) bescheinigen lassen
  Das heisst : Personenangaben werden mit dem Schlüsselpaar gekoppelt (Elektronischer Ausweis), ausgestellt von einer vertrauenswürdigen Instanz **TC** (=**T**rust **C**enter) oder CA

Digitale Signatur mit «RSA»

Public Key Infrastruktur:

Aufgaben von TC's bzw. CA's (X.509)

- **Zertifikate ausstellen** : Korrekte Identifikation des Teilnehmers,
  Zertifizieren von User, Server, Sub CA's
  Erstellung des Zertifikates durch digitale Signatur über Identifikationsdaten
  und öffentlichen Schlüssel eines Teilnehmers

- Bei Ausgabe eines Zertifikates an einen Teilnehmer ist dieser über Funktionalität
  und Gefahren von zertifizierten Signaturschlüsseln zu unterrichten

- **Veröffentlichen** der Public-Keys der User

- Publizieren eigenes Zertifikat

- **Verwalten bzw. Archivierung** angelaufener Zertifikate

- Zertifikate zurückziehen oder für ungültig erklären

- Festlegung der Gültigkeitsdauer von Zertifikaten

- Zeitstempeldienst: Absicherung im Falle des Diebstahls des geheimen Schlüssels.
  Nachweis einer zeitpunktsbezogenen Willensbekundung.
  Nachweis und Sicherheit, dass die digitale Signatur nicht nach Ablauf der Gültigkeit
  des Zertifikates erstellt wurde.

Digitale Signatur mit «RSA»

RSA-Schwachstelle: Der Geburtstagsangriff

Eigentlich sollte Dokument und dazugehöriger Hashwert einmalig sein.

Dem ist leider nicht ganz so. Nach langem PC-unterstützten Suchen ist es möglich, zwei unterschiedliche Dokumente mit gleichem Hashwert zu finden!

1. Mallory erstellt zwei Versionen eines Dokumentes „Guter Text: Alice an Bob“ und „Böser Text: Alice an Mallory“
2. Mallory erstellt von beiden Dokumenten (Gut und Böse) je verschiedene Varianten. Der jeweilige Inhalt wird dabei geringfügig, dh. von Auge kaum erkennbar, abgeändert (zB. einfügen von Leerschläge etc.)
3. Mallory sucht „Gut“ und „Böse“ Varianten mit demselben Hash-wert (Die Wahrscheinlichkeit für ein Treffer ist relativ hoch!)
4. Mallory legt Alice die gefundene Variante von „Guter Text“ zur Unter-schrift vor.
5. Alice unterschreibt die „Guter Text: Alice an Bob“ für Bob
6. Mallory trennt nun die Signatur von „Guter Text“ ab und fügt sie „Böser Text: Alice an Mallory“ an.
7. „Böser Text: Alice an Mallory“ ist nun ebenfalls gültig !

Digitale Signatur mit «RSA»

RSA-Schwachstelle: Chosen Cyphertext

1. Mallory fängt verschlüsselte Nachricht an Bob ab und besorgt sich den Public-Key von Bob.
2. Mallory wählt Zufallszahl r (r<n und teilerfremd zu n)
3. Mallory : $x=r^e \bmod n$ (e=Public-Key von Bob)
4. Mallory : $y=x * c \bmod n$ (c=Nachricht)
5. Mallory überredet Bob dazu, die errechnete Nachricht y digital zu signieren.
6. Bob : $u=y^d \bmod n$ (d=Private Key von Bob)
7. Mallory : $r^{-1} * u \bmod n = r^{-1} * y^d \bmod n$
   $= r^{-1} * x^d * c^d \bmod n$
   $= r^{-1} * (r^e)^d * c^d \bmod n$
   $= r^{-1} * r * c^d \bmod n$
8. Die Exponenten e und d heben sich gegenseitig auf wie auch r und r^{-1}. Es bleibt übrig : $c^d \bmod n$ >> Die Klartextnachricht !!!

Digitale Signatur mit «RSA»

Massnahmen gegen RSA-Schwachstellen:

Geburtstagsangriff :

Unterschreiben Sie niemals ein Dokument, (auch wenn es für sie im Klartext abgefasst ist), das sie nicht selber verfasst haben. Es sei denn, sie nehmen vor der Unterzeichnung einige subtile Aenderungen vor.
ZB. Vor der Unterzeichnung Einfügen von Leerzeichen; Damit ändern sie wiederum den Haschwert der ihnen vorgelegten Daten und machen den Geburtstagsangriff zunichte.

Chosen Cyphertext :

Unterschreiben sie nie irgendwelche binären Dateien unbekannten Inhalts mit ihrem privaten Schlüssel –
es könnte sich um einen Chosen-Ciphertext-Angriff handeln.
(=Man in the middle-Attack)

Zusammenfassung

Symmetrische Verschlüsselung (Secret Key)

- ein geheimer Schlüssel steuert Chiffrieren und Dechiffrieren
- primäres Ziel : Vertraulichkeit
- Sogenannt klassische Kryptographie.

Asymmetrische Verschlüsselung (Public/Privat Key)

- Chiffrieren und Dechiffrieren mit zwei verschiedenen Schlüsseln, die ein Schlüsselpaar bilden.
- Öffentlicher Schlüssel (public key, Chiffrierschlüssel) **ver**schlüsselt, wird öffentlich bekannt gemacht und beliebig verteilt.
- Privater Schlüssel (private key, Dechiffrierschlüssel) **ent**schlüsselt, liegt nur dem Empfänger vor und ist geheim.
- Nachrichten, die mit dem öffentlichen Schlüssel des Empfängers verschlüsselt wurden, können ausschliesslich mit dessen privatem Schlüssel entschlüsselt werden.

Zusammenfassung

Asymmetrische Verschlüsselung (Public/Private Key)

- Sehr sicher (“hacken” scheitert an der Rechnerkapazität) nur 2 Schlüssel pro Teilnehmer
- Wer erzeugt Schlüsselpaare ? (Authentizität)

RSA

- Benannt nach Rivest, Shamir, Adleman
- Öffentlicher und privater Schlüssel hängen von einem Primzahlenpaar ab
- Sicherheit von RSA beruht auf speziellen mathematischen Funktionen, die nicht umkehrbar sind.
- Gebräuchliche Schlüssellängen :
  1024-bit (2004), 2048-bit, 3072-bit, 4096-bit
- Sowohl für Verschlüsselung als auch für digitale Signaturen