Leibniz Gemeinschaft

IPN
Leibniz-Institut für die Pädagogik der Naturwissenschaften und Mathematik

Asymmetrische Verschlüsselung

Bisherigen Verfahren

- Sender und Empfänger benötigen den gleichen Schlüssel.
- „Symmetrische“ Verschlüsselungsverfahren
- Wenn der Schlüssel sicher übertragen werden kann, dann auch die Nachricht.

Ergänzung der symmetrischen Verfahren

- Verfahren, das keinen Schlüsseltausch braucht
- Verfahren, das mit einem Schlüssel verschlüsselt, mit einem anderen entschlüsselt
- Verfahren, bei dem Sender und Empfänger den Schlüssel gemeinsam erstellen

Ergänzung der symmetrischen Verfahren

- Verfahren, das keinen Schlüsseltausch braucht
- Verfahren, das mit einem Schlüssel verschlüsselt, mit einem anderen entschlüsselt
- Verfahren, bei dem Sender und Empfänger den Schlüssel gemeinsam erstellen

Verfahren ohne Schlüsseltausch

- Sender verschlüsselt Nachricht mit eigenem Schlüssel, sendet an Empfänger.
- Empfänger verschlüsselt Nachricht mit eigenem Schlüssel, sendet an Sender.
- Sender entschlüsselt Nachricht, sendet an Empfänger.
- Empfänger entschlüsselt Nachricht und erhält Klartext.

Probleme

- Hoher Übertragungs-Aufwand
- Die Reihenfolge ist wichtig!
  - Beispiel Permutations-Verfahren (Skytale)

Reihenfolge wichtig

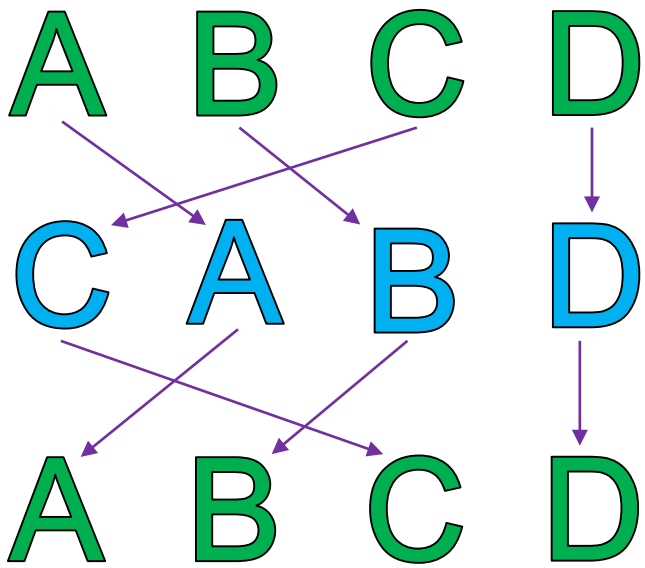
Nachricht

Verschlüsselung Sender

Chiffre

Entschlüsselung Sender

Klartext



Reihenfolge wichtig

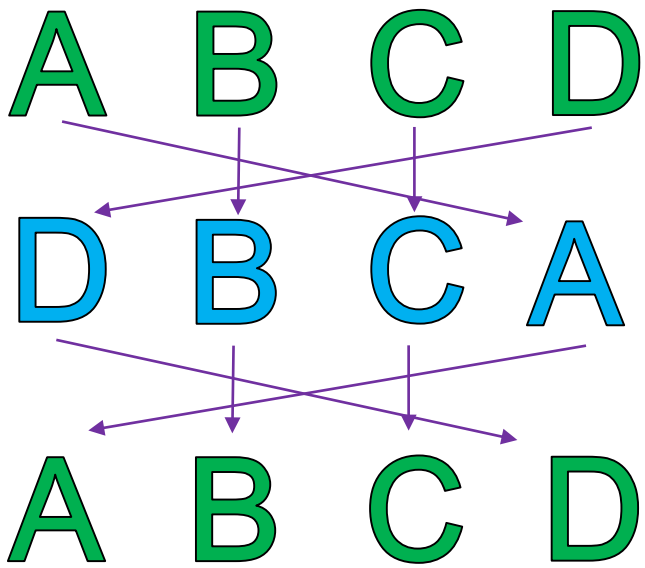
Nachricht

Verschlüsselung Empfänger

Chiffre

Entschlüsselung Empfänger

Klartext



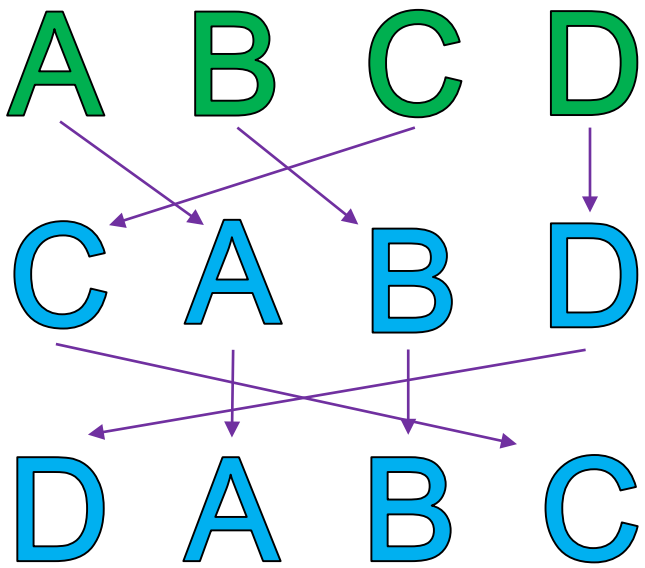
Reihenfolge wichtig

Nachricht

Verschlüsselung Sender

Verschlüsselung Empfänger

Chiffre



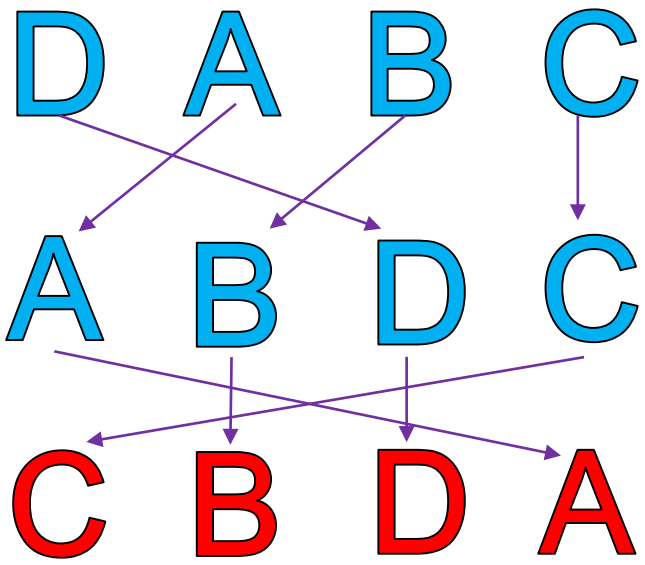
Reihenfolge wichtig

Chiffre

Entschlüsselung Sender

Entschlüsselung Empfänger

Nicht der Klartext



Ergänzung der symmetrischen Verfahren

- Verfahren, das keinen Schlüsseltausch braucht
- Verfahren, das mit einem Schlüssel verschlüsselt, mit einem anderen entschlüsselt
- Verfahren, bei dem Sender und Empfänger den Schlüssel gemeinsam erstellen

Public-Key-Verfahren

- Jeder Empfänger besitzt zwei Schlüssel
- Einen Öffentlichen und einen Privaten

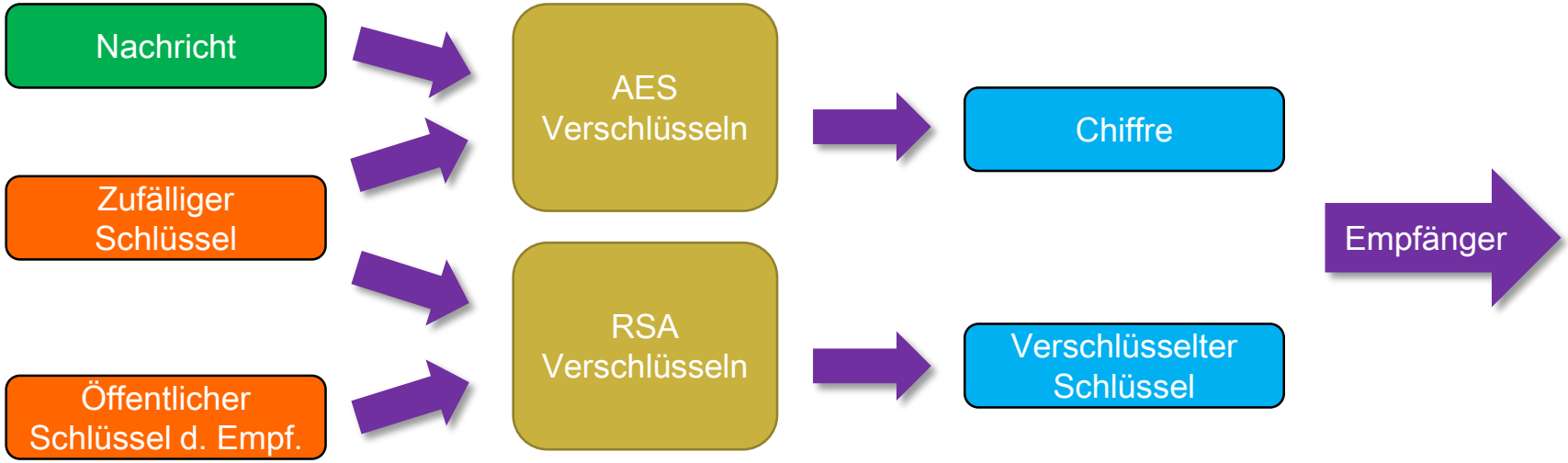
- Öffentlicher Schlüssel:
  - Für jeden zugänglich
  - Vom Sender zum Verschlüsseln genutzt

- Privater Schlüssel:
  - Nur dem Empfänger bekannt
  - Vom Empfänger zum Entschlüsseln genutzt

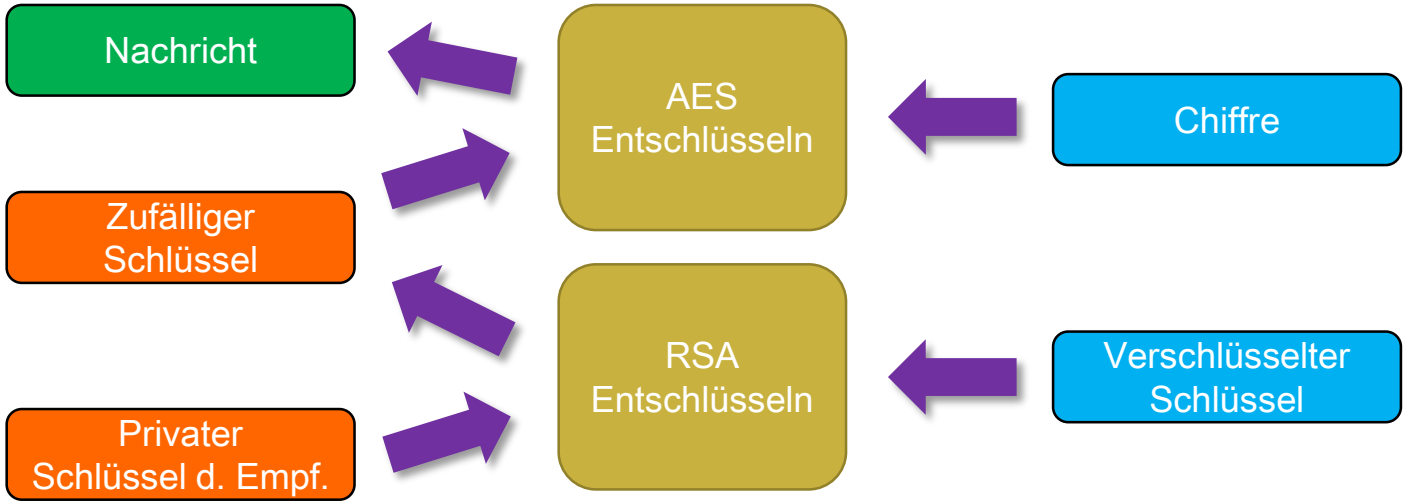
RSA

- Das am weitesten verbreitete asymmetrische Verfahren
- 1977 (Rivest & Shamir)
- Sehr rechenaufwändig, deshalb nur zum übertragen des Schlüssels benutzt

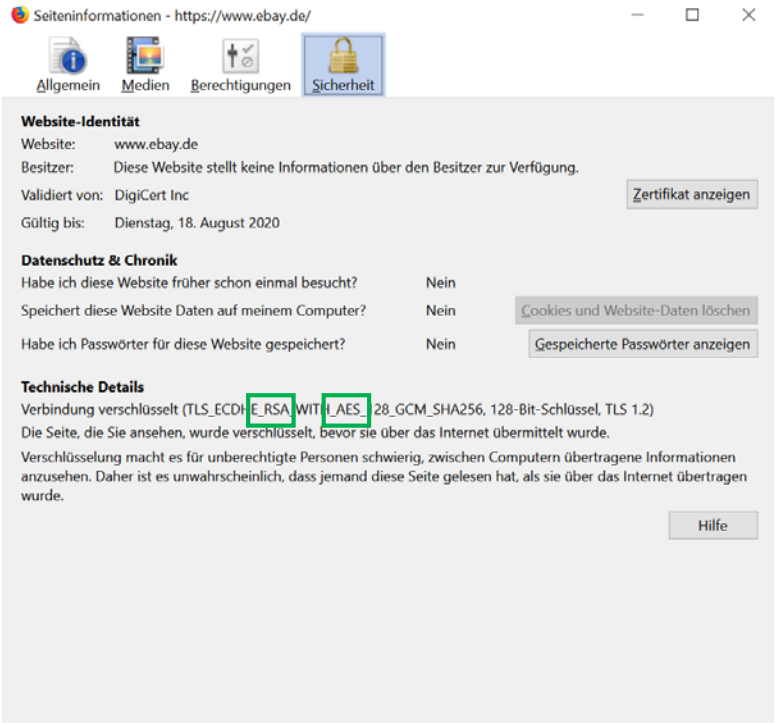
Hybride Verschlüsselung



Hybride Verschlüsselung



Hybride Verschlüsselung



Ergänzung der symmetrischen Verfahren

- Verfahren, das keinen Schlüsseltausch braucht
- Verfahren, das mit einem Schlüssel verschlüsselt, mit einem anderen entschlüsselt
- Verfahren, bei dem Sender und Empfänger den Schlüssel gemeinsam erstellen

Diffie-Hellman-Schlüsseltausch

- Zwei Parteien machen einen Schlüssel ab
- Der Schlüssel selber muss nicht übertragen werden
- Es gibt eine öffentliche Information

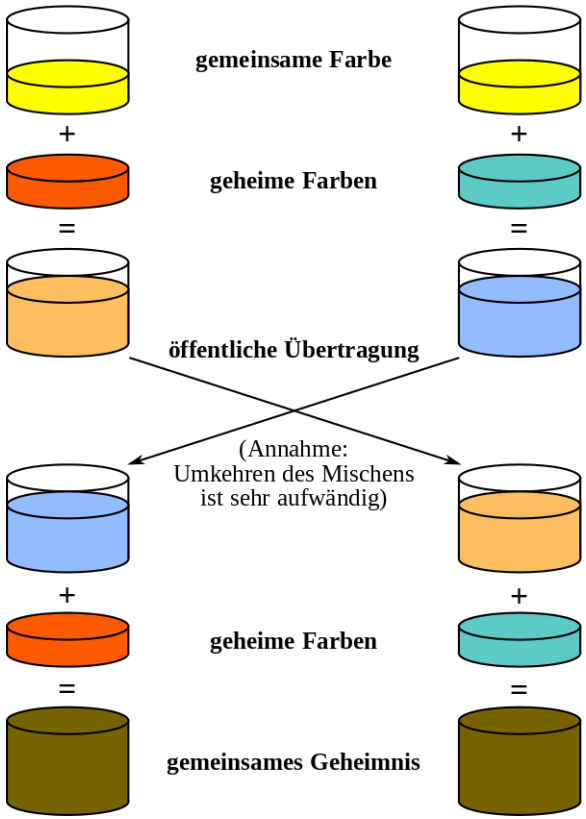
Diffie-Hellman-Schlüsseltausch

- Beide haben eine geheime Information
- Aus öffentlicher und geheimer Information wird ein Wert berechnet
- Dieser Wert wird übertragen und liefert keinen Aufschluss über geheime Informationen

Diffie-Hellman-Schlüsseltausch

- Aus dem berechneten Wert des anderen und der eigenen geheimen Information wird Schlüssel berechnet
- Beide Seiten liefern gleichen Schlüssel

Veranschaulichung Farben mischen



Veranschaulichung Suppe würzen

- Eine gemeinsame Grundsuppe
- Beide haben eigene Gewürzmischung
- Einer würzt die Grundsuppe und gibt sie an den anderen
- Der andere macht das Gleiche

Veranschaulichung Suppe würzen

- Beide würzen, die vom anderen erhaltene Suppe mit der eigenen Gewürzmischung
- Beide Suppen schmecken gleich

Diffie-Hellman-Schlüsseltausch

- Es gibt eine öffentliche Information
- Beide haben eine geheime Information
- Aus öffentlicher und geheimer Information wird ein Wert berechnet
- Dieser Wert wird übertragen und liefert keinen Aufschluss über geheime Informationen

Diffie-Hellman-Schlüsseltausch

- **Mathematisch**: Funktion gesucht, die einfach zu berechnen, aber
- schwer rückgängig zu machen ist.

- Beispiel: Was ist x?
  - Einfach: $23^3 \pmod{13} = x$
  - Schwer: $23^x \pmod{13} = 11$

Potenzen

- $26 \cdot 26 \cdot 26 \cdot 26 \cdot 26 \cdot 26 \cdot 26$ (Vigenère)
- Schreibweise: 26^7

- $2^4 = 2 \cdot 2 \cdot 2 \cdot 2 = 16$
- $5^2 = 5 \cdot 5 = 25$
- $3^5 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 9 \cdot 9 \cdot 3 = 81 \cdot 3 = 241$

Diskrete Logarithmus

- Beispiel:
  - Einfach: $23^3 \pmod{13} = 12$
  - Schwer: $23^x \pmod{13} = 11$

- Es gibt kein (bekanntes) Verfahren x schnell zu berechnen
- Schnellste: alle ausprobieren

Auftrag Nr. 1

- Finde ein x mit: $2^x \pmod{13} = 7$

- Nutze die Funktion `` `pow( * , * , * )` ``
- `` `pow(2,3,13)` `` ergibt $2^3 \pmod{13}$
- **Lösung**: x = 11

Rechenregeln

- $(2^4)^3 = (2 \cdot 2 \cdot 2 \cdot 2)^3$

  $= (2 \cdot 2 \cdot 2 \cdot 2) \cdot (2 \cdot 2 \cdot 2 \cdot 2) \cdot (2 \cdot 2 \cdot 2 \cdot 2)$

  $= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$

  $= 2^{12} = 2^{4 \cdot 3}$

Rechenregeln

- $(7^2)^4 = (7 \cdot 7)^4 = (7 \cdot 7) \cdot (7 \cdot 7) \cdot (7 \cdot 7) \cdot (7 \cdot 7)$

  $= 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7$

  $= 7^8 = 7^{2 \cdot 4}$

- $(25^{12})^4 =$

Rechenregeln

- $(7^2)^4 = (7 \cdot 7)^4 = (7 \cdot 7) \cdot (7 \cdot 7) \cdot (7 \cdot 7) \cdot (7 \cdot 7)$

  $= 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7$

  $= 7^8 = 7^{2 \cdot 4}$

- $(25^{12})^4 = 25^{48}$
- $(32^8)^9 =$

Rechenregeln

- $(7^2)^4 = (7 \cdot 7)^4 = (7 \cdot 7) \cdot (7 \cdot 7) \cdot (7 \cdot 7) \cdot (7 \cdot 7)$
  $= 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7$
  $= 7^8 = 7^{2 \cdot 4}$
- $(25^{12})^4 = 25^{48}$
- $(32^8)^9 = 32^{72}$

Diffie-Hellmann-Schlüsseltausch

Beispiel:

- Beide wählen gemeinsame Primzahl: p = 13 und eine Zahl die kleiner als p ist: g = 2.
- Jeder wählt eine zufällige Zahl, die kleiner als 13 ist. Dies ist der private Schlüssel.
- Person 1: 5
- Person 2: 8
- und berechnet „2 hoch privater Schlüssel“, also:

Diffie-Hellmann-Schlüsseltausch

Beispiel:

- Person 1: 2^5 (mod13) = 32 (mod13) = 6
- Person 2: 2^8 (mod13) = 256 (mod13) = 9
- Person 2 erhält von Person 1: 6
- Person 1 erhält von Person 2: 9
- Beide rechnen erhaltenen Wert „hoch privaten Schlüssel“
- Person 1 : 9^5 (mod13) = 3
- Person 2 : 6^8 (mod13) = 3

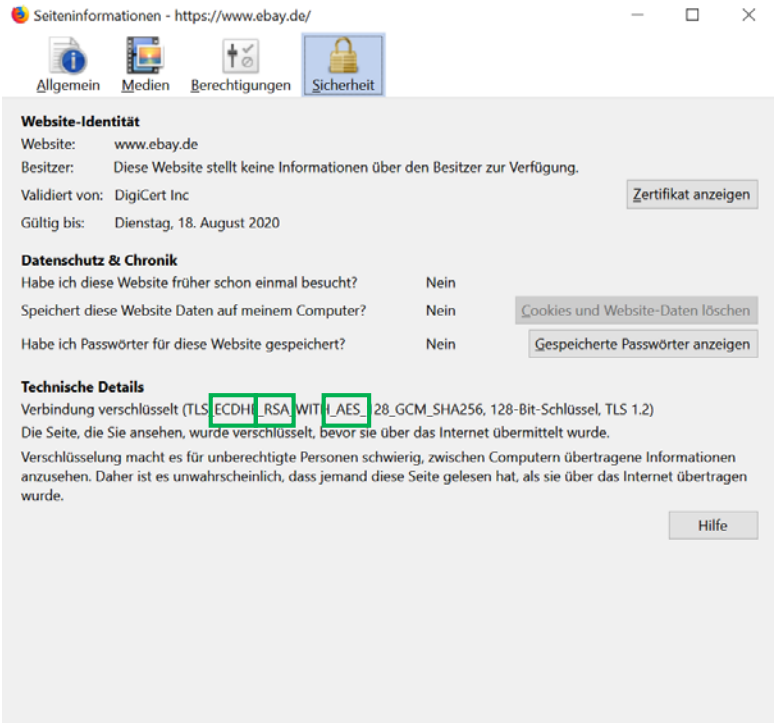
Diffie-Hellmann-Schlüsseltausch

Beispiel:

- $2^5 \pmod{13} = 32 \pmod{13} = 6$
- $2^8 \pmod{13} = 256 \pmod{13} = 9$

- $6^8 \pmod{13} = (2^5)^8 \pmod{13} = 2^{5 \cdot 8} \pmod{13} = 2^{40} \pmod{13}$
- $9^5 \pmod{13} = (2^8)^5 \pmod{13} = 2^{8 \cdot 5} \pmod{13} = 2^{40} \pmod{13}$

Hybride Verschlüsselung



Zusammenfassung

- Asymmetrische Verfahren benötigen keinen Schlüsseltausch
- Im Einsatz: RSA und Diffie-Hellman
- Stützen sich auf Exponentialfunktionen

- Asymmetrische Verfahren sind aufwändig, werden deshalb zusammen mit Symmetrischen (AES) verwendet

Hast du eine Frage, einen Fehler gefunden oder sonstige Anregungen? Melde dich bei uns!

Unter karrasch@leibniz-ipn.de oder info@panama-project.eu