Eulersche phi-funktion e(x) gibt an, wie viele Zahlen y es gibt, die zu x teilerfremd sind.

Teilerfremd bedeutet, dass x und y nur den gemeinsamen Teiler 1 haben.

Themen:

Diffie-Hellmann:

Zweck Robin

Aufbau Felix

Beispiel Kristof

Anwendung Leon

Sicherheit Jenny

RSA:

Zweck Robin

Aufbau Leon

Beispiel Kristof

Anwendung Jenny

Sicherheit Felix

Diffie-Hellmann

Zweck:

Erzeugung eines geheimen Schlüssels und Austausch dieses Schlüssels über ein unsicheres Medium. Dies kann bei einem sysmmetrischen Kryptosystem eingesetzt werden. Dieser Schlüssel kann dann zur Ver-/Entschlüsselung von verschickten Texten genutzt werden. In Verbindung mit einer ROT-Verschlüsselung wäre der Austausch des entsprechenden Schlüssels denkbar. (Mitgabe des Schlüssels ‚3‘ bei einer ROT3-Verschlüsselung).

Nähere Erklärung zu:

* Dem wirklichen Sinn
* Symmetrischem Kryptosystem
* ROT-Verschlüsselung (nur ein-zwei Worte)

Aufbau:

Mit Primzahlen, Primitivwurzeln (Erklärung) und Restberechnungen (Modulo) werden Zahlen berechnet, die auch über unsichere Medien übertragen werden können. Mit jeweiligen Formeln können Absender und Empfänger mit diesen Zahlen auf einen Schlüssel schließen, der bei beiden Personen gleich ist.

Nähere Erklärung zu:

* Dem Aufbau (Formeln etc.)
* Gleichheit der Ver-/Entschlüsselung

Beispiel:

Grundsätzliches Beispiel, um grob die Funktionsweise zu erläutern. Möglicherweise mit Einbeziehung der Klasse bei einfachen Rechnungen. Nicht zu detailliert. Wenn zu viele Zahlen etc. vorkommen, verwirrt das nur.

Nähere Erklärung zu:

* Gleichheit der Ver-/Entschlüsselung (am Beispiel direkt zu zeigen).
* Klar machen, welcher Teil verschlüsselt ist und welcher nicht

Anwendung:

Laut Quellen: VPN. Informationen müssen noch gefunden werden.

Nähere Erklärung zu:

* VPN
* Zusammenspiel

Sicherheit:

Anfällig gegen ‚Man-in-the-middle‘-Angriff. Dieser ‚Man‘ kann die Schlüssel austauschen und die Nachrichten verfälschen.

* + Alice ----- Man-in-the-Middle ----- Bob
  + Situation: Alice und Bob wollen ihre Schlüssel austauschen und eine Person hat sich dazwischen geschaltet

Nähere Erklärung zu:

* Schlüssel ersetzen
  + Person empfängt die beiden Schlüssel, verändert (zweimal Diffie-Hellman-Schlüsselaustausch ausführen) diese und sendet sie weiter an Bob und Alice
* Nachricht verfälschen
  + Person empfängt die Nachrichten liest, verhindert oder verändert diese sogar und sendet sie eventuell an den jeweiligen Empfänger weiter

RSA:

Zweck (Wozu dient das Kryptoverfahren? Was ermöglicht das Verfahren?)

Aufbau (Wie ist das System prinzipiell aufgebaut? Was sind grundlegende Aspekte?)

Beispiel (Ein praktisches Beispiel, das die Anwendung an einem einfachen Beispiel zeigt)

Anwendung (Wo wird oder wurde dieses Verfahren real eingesetzt?)

Sicherheit (Wie sicher ist das Verfahren? Was sind Schwachstellen? Gibt es erfolgreiche Angriffe?)

1.

asymmetrisches kryptographisches Verfahren

Verschlüsselung als auch digitale Signatur

Einwegfunktionen

private Schlüssel(Falltür) wird geheim gehalten und kann nur mit extrem hohem Aufwand aus dem öffentlichen Schlüssel berechnet werden

beispiel: 5\*6 ist leicht zu berechnen, aber von 30 auf 5 zu schließen, ohne die Information 6 (Falltür)

2.

Schlüsselpaar

privaten Schlüssel zum Entschlüsseln oder Signieren

öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft.

--> TODO:

Formeln genau und Rechnung

3.

4.

Anwendung

* Pretty Good Privacy (PGP)
  + Bekanntes Verschlüsselungsprogramm
  + Benutzt RSA-Algorithmus
  + Ist so siehcre, dass es verboten war das Programm von Amerika nach Europa zu exportieren, da es unter das militärische Gesetzt zur Spionageabwehr fiel
* Chipkarten
  + Spezielle RSA-Chipkarten, die beispielsweise einen PIN mit dem RSA-Algorithmus verschlüsseln
* Bankenwesen
  + Z.B. Verschlüsselung von Geheimzahlen
* Verschleierung von Pay-TV-Programmen
* Verschlüsselung von Mobilfunknetzen
* Verschlüsselung bei Geheimdiensten

5.

Die erste Möglichkeit ergibt sich durch das Faktorisieren von n in die beiden Primzahlen p und q, da mit p, q und e (der geheime Schlüssel d) berechnet werden kann.

Für dieses Problem ist keine hinreichend schnelle mathematische Möglichkeit bekannt.

Attacke beim Austausch des öffentlichen Schlüssels:

Wenn ein Anwender X den Anwendern A, B beim Schlüsseltausch vorspielt jeweils der andere zu sein, und beiden seinen öffentlichen Schlüssel zuspielt, so kann er ihre Nachrichten lesen.

Zur Lösung dieses Problems, der Vorspiegelung falscher Tatsachen, wurden sogenannte Certification Authorities gegründet, welche garantieren, dass ein öffentlicher Schlüssel B0 den A von B anfordert auch tatsächtlich der öffentliche Schlüssel von B ist.

Eine weitere Möglichkeit zur Lösung dieses Problems der Schlüssel-Authorities wäre, einen sogenannten Fingerprint des öffentlichen Schlüssels über einen sicheren Kanal auszutauschen, wie zum Beispiel das Telefon.

Die Sicherheit des Verfahrens basiert auf dem Problem, dass eine große, ganze Zahl in ihre Primfaktoren zerlegt werden muß, dies bedeutet, dass die Schlüssellänge nicht zu klein gewählt werden darf.

Ein Schlüssel der Länge 512 Bit, der zu Zeit noch als Standard-Sicherheit gilt, wurde in nur 3 Tagen geknackt. Es sollte also mindestens eine Schlüssellänge von 1024 Bit (Militär-Standard) oder noch besser 2048 Bit gewählt werden.

--> Das heißt: Je größer die Primzahl desto unverhälnissmäßiger wird der Zeitaufwand