LU05d - Die Hybrid-Verschlüsselung

Lernziele

- Grund nennen können, warum es die Hybrid-Verschlüsselung braucht.
- Prozessablauf beim Ver-und Entschlüsseln der Hybrid-Verschlüsselung darlegen können.

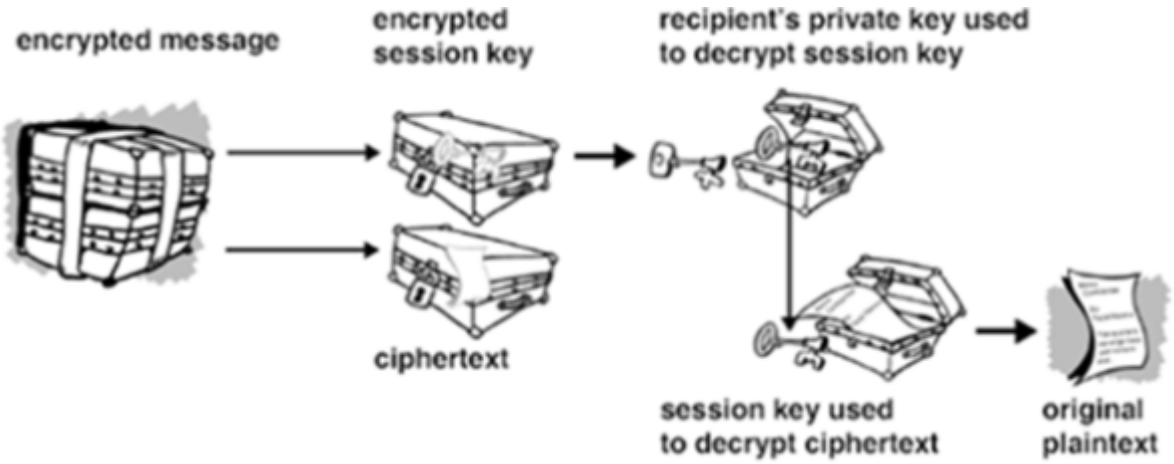
Einleitung

Die symmetrische (Schlüsselmanagement, fehleranfällig), wie auch die asymmetrische Verschlüsselung (Rechenintensiv) hat jede für sich Nachteile. Die Hybdrid-Verschlüsselung kombiniert die Vorteile beider Systeme mit grossem Erfolg.

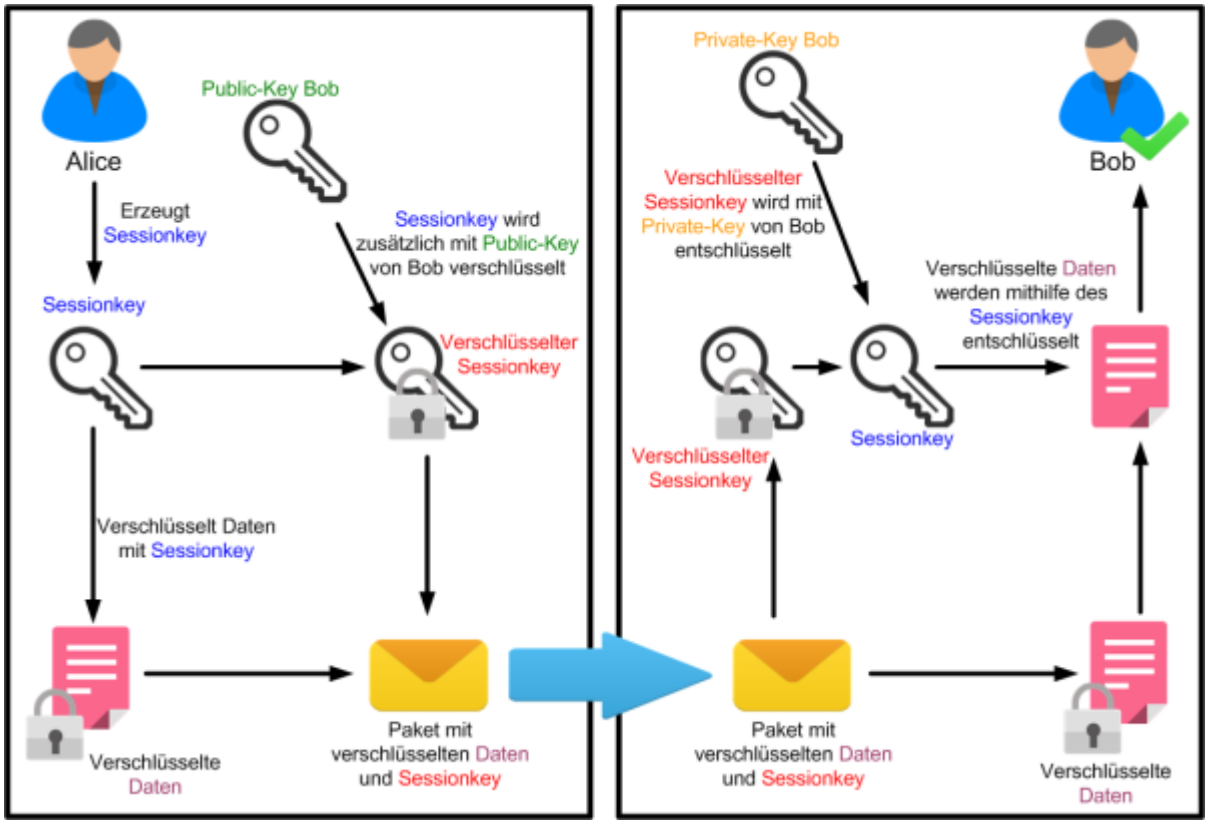
Die Hybrid-Verschlüsselung

Auf Grund der genannten Nachteile von asymmetrischen Verfahren werden im Allgemeinen nicht ganze Meldungen mit diesem Verfahren verschlüsselt. Man behilft sich so, dass die Nachricht mit einem symmetrischen Verfahren verschlüsselt wird. Der Schlüssel dazu, welcher speziell für diese Nachricht erzeugt wurde, muss aber natürlich dem Empfänger der Nachricht mitgeteilt werden. Dazu wird er mit dessen öffentlichem Schlüssel verschlüsselt und mit dem Ciphretext mitgeschickt.

Der Empfänger muss dann zuerst mit seinem privaten Schlüssel den symmetrischen Schlüssel „wieder auspacken“, um dann damit die Nachricht zu entschlüsseln.



Das nachfolgende Ablaufdiagramm zeigt die Funktionsweise der Hybrid-Verschlüsselung



Quellen

- https://xinux.net/index.php/Hybride_Verschl%C3%BCsselung
