

LU05d - Die Hybrid-Verschlüsselung

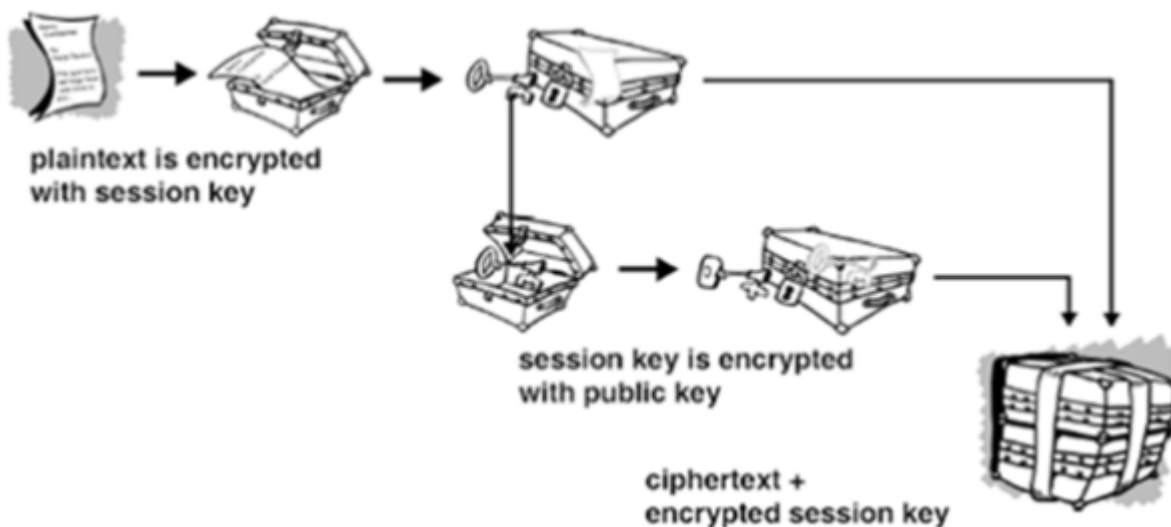
Lernziele

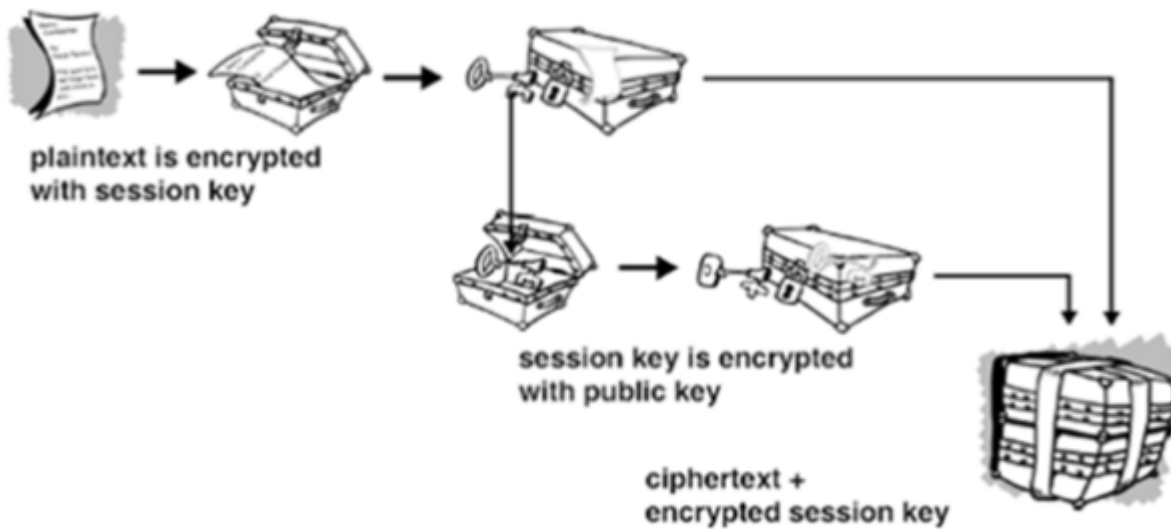
Einleitung

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

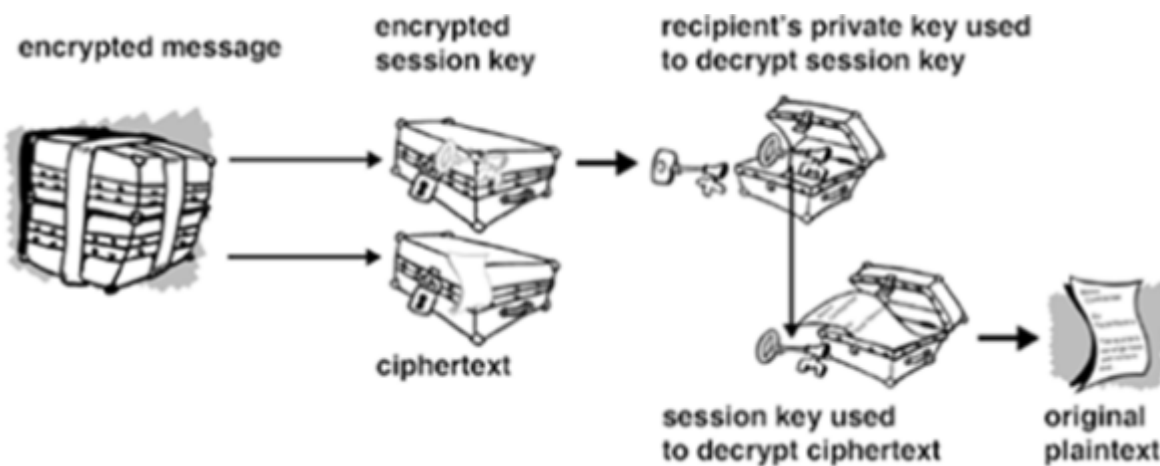
Die Hybrid-Verschlüsselung

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 Ciphertext mitgeschickt.





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



Volkan Demir

From:

<https://wiki.bzz.ch/> - **BZZ - Modulwiki**

Permanent link:

<https://wiki.bzz.ch/modul/m183/learningunits/lu05/04?rev=1755083232>

Last update: **2025/08/13 13:07**

