Stationenarbeit "moderne" Verschlüsselungsverfahren

Arbeitsauftrag

Lege zuerst eine eigene Unterseite `krypto:moderneverfahren:start` in deinem persönlichen Wikibereich an. Lege anschließend für **jede Station eine Seite** an, auf die du die Fragen kopierst und mit deinen Antworten ergänzt.

Station A: Symmetrische Verfahren

Führe eine Recherche über die drei Verschlüsselungsverfahren DES, AES und IDEA durch. Beantworte die folgenden Fragen. Achte darauf, dass deine Antworten auch Verweise zu den Quellen enthalten, aus denen du deine Informationen bezogen hast.

Allgemein

1. Was ist ein *symmetrisches* Verschlüsselungsverfahren?
2. Was ist ein *Blockschiffre* (Blockverschlüsselung)? Was bedeutet in diesem Zusammenhang z.B. die Angabe "64 Bit"?
3. Was ist ein *rundenbasiertes* Verschlüsselungsverfahren? Was ist ein Rundenschlüssel?

DES

1. Wofür steht die Abkürzung "DES"? Wann und durch wen wurde dieses Verschlüsselungsverfahren veröffentlicht?
2. Wann war die erste erfolgreiche Kryptoanalyse von DES? Von welcher Art war der Angriff?
3. Wie groß ist die *Blockgröße* bei DES? Wie groß ist ein Schlüssel (Schlüssellänge)? Wie viele verschiendene Schlüssel gibt es?
4. Was ist *Triple-DES*? Warum wird es verwendet?

AES

1. Warum wurde AES(-Rijndael) entwickelt? Beschreibe kurz die Entstehungsgeschichte.
2. Was sind die wesentlichen Unterschiede zwischen AES und DES?

Probiere den AES Algorithmus bei Crytool-Online aus: https://www.cryptool.org/de/cto-highlights/aes

IDEA

1. Wer hat das IDEA-Verfahren entwicklet? In welchem Jahr wurde es vorgestellt?
2. Wie lang ist ein IDEA-Schlüssel?
3. Welchen rechtliche Unterschied gibt es zwischen AES bzw. DES und IDEA?

Station B: Asymmetrische Verschlüsselungsverfahren

Ein lohnender Startpunkt ist die Facharbeit von Matthias Deininger

1. Was ist der grundlegende Unterschied zwischen den bisher kennen gelernten Verfahren und asymmetrischen Verfahren? Erkläre in diesem Zusammenhang den Begriff "Public-Key-Kryptographie".
2. Welches grundlegende Problem der symmetrischen Kryptoverfahren löst die asymetrische Kryptographie?
3. Bei asymmetrischen Verfahren betrachtet man häufig das sogenannte "Alice-Bob-Mallory-Szenario". Hierbei will Alice eine Nachricht an Bob verschicken und verschlüsselt zu diesem Zweck die Nachricht. Mallory (oder Eve) ist ein(e) Angreifer(in), der/die die Nachricht entschlüsseln will. (Weitere Infos)
4. Wenn **S_oeffentlich** der öffentliche Schlüssel von Bob ist und **S_geheim** sein geheimer (oder privater) Schlüssel, wie müssen Alice und Bob dann Schritt für Schtritt vorgehen, damit Alice eine verschlüsselte Nachricht an Bob schreiben kann und Bob diese auch entschlüsseln kann?
5. Ein Beispiel für ein asymmetrisches Verschlüsselungsverfahren ist der sogenannte RSA-Algorithmus. Wer hat dieses Verschlüsselungsverfahren entwickelt? In welchem Jahr wurde es vorgestellt?
6. Worauf basiert das Funktionsprinzip von RSA? Wie groß müssen (zur Zeit) die verwendeten Zahlen sein?
7. Asymmetrische Verfahren scheinen eine sehr hohe Sicherheit zu bieten. Warum verwendet man solche Verfahren dennoch nicht standardmäßig? Erkläre hierbei den Begriff "hybride Verschlüsselung"

Du kannst den RSA Algorithmus ebenfalls bei Cryptool-Online ausprobieren:
https://www.cryptool.org/de/cto-highlights/rsa-schritt-fuer-schritt

1. Spiele das Verfahren durch und notiere dir die einzelnen Schritte des Beispiels
    1. Was ist der Öffentliche Schlüssel (woraus besteht er)?
    2. Was ist der private Schlüssel (woraus besteht er)?
    3. Wie wird verschlüsselt?
    4. Wie wird entschlüsselt?

Lies dir RSA Step by Step durch und vollziehe das Verfahren nach (Du kannst auf der Konsole den Rechner bc verwenden, Modulo kann mit % berechnet werden).

- Welche Schwierigkeiten siehst du im Alltagseinsatz?
- Mache dir klar, dass man öffentlichen und privaten Schlüssel problemlos vertauschen kann (Rechne nach!).

Station C: Gesellschaftliche Aspekte der Kryptographie

1. Das DES-Verfahren (siehe Station A) wurde seit seiner Entwicklung stark kritisiert. Begründe diese Kritik.
2. Was ist "Tempora/Prism"? Was geschieht in diesem Zusammenhang mutmaßlich mit verschlüsselter Kommunikation im Internet und warum?
3. Wofür steht die Abkürzung PGP? Informiere dich über den Autor und die Beweggründe für die

Erfindung von PGP.
4. Finde Argumente, die **für** eine frei zugänglich starke Verschlüsselungstechnik für jedermann sprechen.
5. Finde Argumente, die **gegen** eine frei zugänglich starke Verschlüsselungstechnik für jedermann sprechen.

Links und Tipps

- http://blogs.helmholtz.de/augenspiegel/2014/09/klar-soweit-no-8-sicher-ist-sicher/