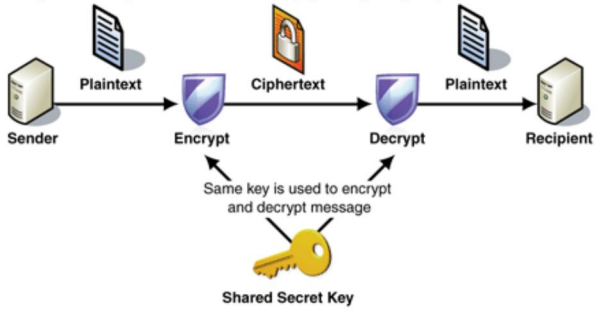
9: XML Security | Control Questions

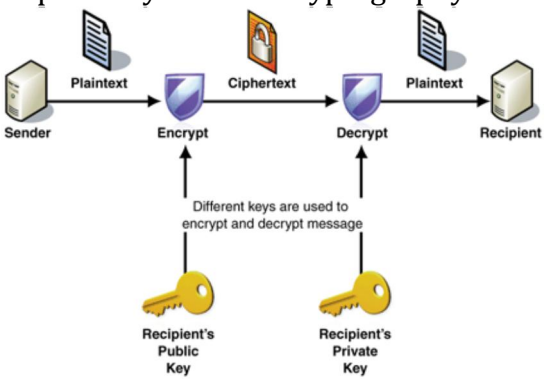
1. Which granularities are distinguished for XML encryption and signatures?
   - *Gesamtes XML-Dokument*
   - *Einzelnes Element in einem XML-Dokument*
   - *Einzelner Inhalt von einem Element in einem XML-Dokument*

2. Explain symmetric cryptography and describe advantages and disadvantages.



Sender und Empfänger benützen den gleichen Key
   - *Nachteil: Schlüsselaustausch muss „sicher" sein*
   - *Vorteil: Sehr Effizient*

3. Explain asymmetric cryptography and describe advantages and disadvantages.



Sender verschlüsselt mit dem Public Key des Empfängers. Der Empfänger entschlüsselt es mit seinem Private-Key.
   - *Nachteil: Aufwendig zum berechnen*
   - *Vorteil: Geheimer Schlüsselaustausch „entfällt"*

4. Explain hybrid cryptography and describe advantages and disadvantages.
   Schlüsselaustausch wird asymmetrisch übertragen. Die Nachrichten werden nachher symmetrisch übermittelt.

5. How can asymmetric cryptography be used for digital signatures? Explain how signatures are created and verified.
   Mit dem privaten Schlüssel signieren. Jeder kann mit dem Public-Key dieser Person die Nachricht überprüfen.

6. Give 3 security properties of digital signatures.
   - *Authentifiziert der Absender*
   - *Die Integrität der Nachricht kann überprüft werden*
   - *Die „nicht ab Streitbarkeit" Bsp. Verträge: Der Absender kann nachträglich die Nachricht nicht „leugnen"*

7. What are the main ingredient in the XML signature format.
   - *verschlüsselte Nachricht*
   - *Verschlüsselung Algorithmus*
   - *Verwendete Schlüssel (Key)*
   - *Kanonisierungsmethode*