Signierte und verschlüsselte Datenübertragung

Du kommunizierst auf verschlüsseltem Weg mit deiner Schule. Deine Schule hat dir nun zwei Nachrichten geschickt und du musst als Empfänger überprüfen, ob mit der Übertragung alles korrekt abgelaufen ist. Sowohl für die Verschlüsselung als auch für die Signatur wurde RSA verwendet.

Die Schule hat zunächst vom Originaltext einen SHA-1-Hash[1] erstellt und diesen mit ihrem eigenen privaten Schlüssel signiert. Anschließend wurde die Klartext-Nachricht mit deinem öffentlichen Schlüssel chiffriert. Die Signatur und die Chiffre werden nun an dich versendet.

Deine Schule sendet dir die beiden folgenden Nachrichten zu:

1.	**Nachricht**: Zg38PQv32c0Fg4PUv21jnRwlFty2EjaCX0XkN0jaeMynblwT/N91n3nELQoTGATоNPrKVxqsX0H7/3ssl9oMuA==	**Signatur**: l4ULM97eiax8GakLINkWKWNyfb4D6yKgBZwcySxq39rL5OWCeZRJE6vL1/gVSj0e3wg3hm3b3OD8VbPhpTFhtQ==

und

2.	**Nachricht**: BmrQ7SmjxlyvtgQffIEOOEoY+TLee8V8xVMOBYic9kLY5dLy1l0yzC7Z7yqD2vD9nGuy+mvmODOUZQTYb5mS2w==	**Signatur**: zNXpKEwZfPG+JffirJOiltZlj2TgGHd9vZyztafBQX9gMwp3mpXLAHPlVDavKF3ttcSRQG9ylfhDh88upDBRtw==

Dabei wurden folgende Public- und Private-Keys verwendet:

Aufgabe

Überprüfe nun beide Nachrichten um sicherzustellen, dass sie wirklich von der Schule gesendet wurden und kein Man-in-the-Middle am Versand beteiligt war. Gehe dazu folgendermaßen vor:

1. Dechiffriere die Nachricht (nutze dazu den korrekten Schlüssel).
2. Berechne den SHA-1-Hash der dechiffrierten Nachricht.
3. Dechiffriere die Signatur, sodass du den Hash der Nachricht vom Sender bekommst.
4. Vergleiche deinen berechneten Hash mit dem Hash des Senders. Nur wenn sie identisch sind, hat tatsächlich die Schule die Nachricht versendet.

Arbeite dazu mit der folgenden Seite: https://www.devglan.com/online-tools/rsa-encryption-decryption Scrolle etwas runter und nutze die interaktive „RSA Decryption“. Bei den Schlüsseln musst du jeweils einstellen, ob es ein Public Key oder Private Key ist. Kopiere die jeweils nötigen Nachrichten/Texte sowie Schlüssel und füge sie dort ein um die eben notierten Schritte 1-4 für beide Nachrichten durchzuführen. **Welche Nachricht wurde möglicherweise abgefangen bzw. manipuliert?**

1)
Hier wird das unsichere SHA-1 genutzt, damit der Hashwert kürzer ist und dadurch hier einfacher eingesetzt werden kann.