Zweiter Übungsblock

Aufgabenbearbeitung fortsetzen

a. Sollten Sie die Aufgaben des ersten Übungsblocks noch nicht abgeschlossen haben, setzen Sie die Bearbeitung dort bitte fort.
b. Bei Schwierigkeiten stellen Sie bitte Fragen

JavaScript Verschlüsselung

a. Binden Sie bitte die Verschlüsselung-Funktionalität aus nachfolgender URL ein: „https://code.google.com/p/crypto-js/“
b. Verschlüsseln Sie bitte die zuvor ausgelesenen Daten der Datei und geben Sie diese Testweise mit „alert();“ aus.

Übertragung simulieren

1. Simulieren Sie zunächst die Übertragung der Daten, indem Sie die JavaScript-Verschlüsselung in einer HTML-Textarea ausgeben lassen und manuell als Input für Ihr PHP-Empfängerskript verwenden.
    a. Verwenden Sie „encodeURI()“ um eine gültige URL zu erhalten. (Verwenden Sie vorerst nur *.txt Dateien)

PHP: Entschlüsselung

a. Entschlüsseln Sie zuvor „übertragenen“ Daten mit Hilfe der PHP-„mcrypt_decrypt()“ und „hash_pbkdf2()“-Funktionen. (hash_pbkdf2() ist ab PHP 5.5.0 verfügbar!)
b. Vergleichen Sie, ob die Daten nach der Entschlüsselung mit dem Original übereinstimmen, indem Sie einen MD5-Hashwert bilden. Sowohl unter JavaScript, wie auch unter PHP sollte der Wert identisch sein. Wenn nicht, ist ein Fehler im Code vorhanden. Versuchen Sie im Fehlerfall den Fehler zu finden.

PHP: Datei erstellen

1. Erstellen Sie mit PHP eine Datei im „Ausgabe“-Ordner. Die Datei soll den entschlüsselten Dateiinhalt enthält und identisch mit der Ausgangsdatei sein.
    a. Der Dateiname spielt zu diesem Zeitpunkt noch keine Rolle.

Zusatzaufgabe

Sollten Sie bereits vor Ende der Übung alle Aufgaben erledigt haben, können Sie nachfolgende Aufgaben umsetzen.

1. Übertragung realisieren
    a. Übertragen Sie die verschlüsselten Daten der Datei an das PHP-Empfängerskript.
    b. Verwenden Sie zur Realisierung der Übertragung die HTML5 XMLHttpRequest API
    c. https://developer.mozilla.org/de/docs/Web/API/XMLHttpRequest
2. Sollten Sie eine funktionierende Übertragung realisiert haben, können Sie damit beginnen größere Dateien zu übertragen, in dem Sie ca. 1MB große Portionen verarbeiten, bis das Ende der Datei erreicht ist.
    a. Fügen Sie in PHP die übertragenen Häppchen wieder zusammen.
    b. Prüfen Sie an ausreichend großen Dateien ob die Zusammensetzung korrekt funktioniert.
    c. Sie können ebenfalls den in JavaScript ermittelten Dateinamen übertragen und die fertig übertragene Datei in PHP korrekt benennen.