IEEE SB Passau Adventskalender 2014

Toggle navigation

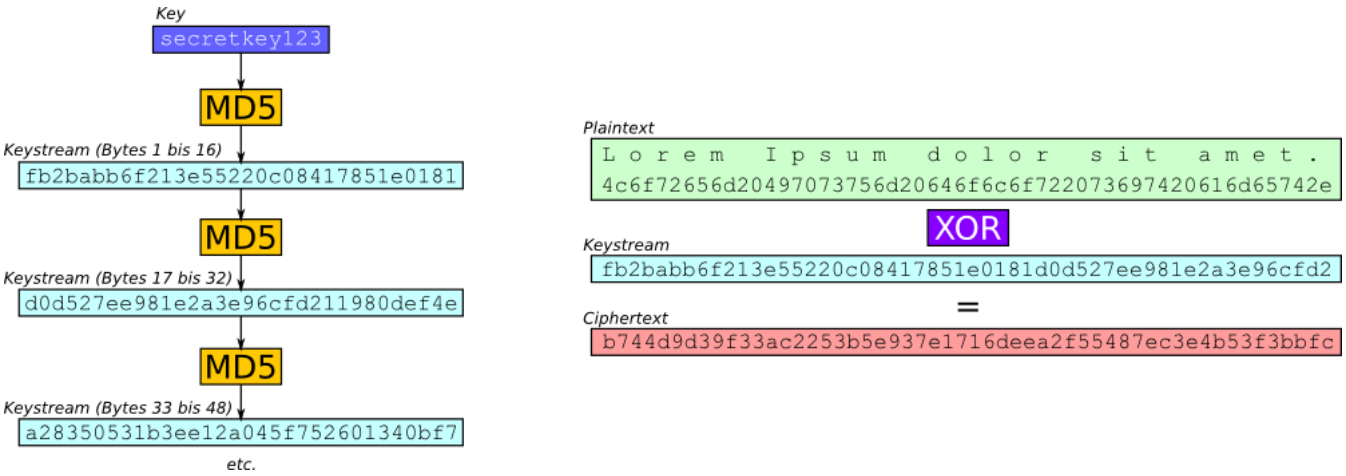
Aufgabe 19: MD5 Stromchiffre

Jakob will seine Daten vor neugierigen Blicken schützen. Er hat die geniale Idee seinen eigenen Verschlüsselungsalgorithmus zu bauen: Er konstruiert eine Stromchiffre.

Zum erzeugen des Schlüsselstroms verwendet er MD5. Die ersten 16 Byte des Schlüsselstroms erzeugt er, indem er die MD5 Funktion auf einen geheimen Schlüssel anwendet. Um Byte 17 bis 32 des Schlüsselstroms zu erzeugen, wendet er die MD5 Funktion auf die ersten 16 Byte des Schlüsselstroms an. Durch wiederholtes Anwenden der MD5 Funktion auf die letzten 16 Byte des Schlüsselstroms, kann Jakob einen beliebig langen Schlüsselstrom erzeugen (in 16 Byte Blöcken).

Um seine Daten zu verschlüsseln, verknüpft er diese Byte für Byte mittels XOR mit dem Schlüsselstrom. Zum Entschlüsseln muss Jakob lediglich den gleichen Vorgang auf die verschlüsselten Daten anwenden.

Die folgende Abbildung verdeutlicht noch einmal die Erzeugung des Schlüsselstroms, sowie die eigentliche Verschlüsselung der Daten:



Kannst du Jakobs Algorithmus knacken? Du hast den Hinweis erhalten, dass Jakob besonders wichtige Informationen am Ende seiner Daten abgespeichert hat. Diese Informationen sind in von den XML-Tags `<message>` und `</message>` umschlossen. Schreibe ein Programm, welches diese Informationen extrahieren kann. Der Rest der Daten interessiert dich nicht.

Eingabe

Die Eingabe besteht aus einer Zeile. Die Zeile besteht aus einer Liste von Bytes, welche Jakobs verschlüsselte Daten darstellen. Jedes Byte ist durch genau zwei hexadezimale Ziffern beschrieben. Die einzelnen Listeneinträge sind durch Leerzeichen voneinander getrennt. Die Länge der Liste ist beschränkt ($200 \leq L \leq 1000$). Als Zeilenvorschub wird \n genutzt.

Ausgabe

Es muss der Inhalt der `message` Tags ausgegeben werden. Die Ausgabe wird mit einem Zeilenvorschub beendet. Als Zeilenvorschub kann \n oder \r\n genutzt werden.

Beispiel

Eingabe

```
52 56 C1 F4 CD F5 D1 41 38 46 4D 17 13 AD 4A 9D 57 3D 0D 98 8E A7 14 88 18 FC 1E 81 B0 AC 11 8C E8 C0 26 16 D0 31 A4 6C 15 05 24 AD FC 09 8A
```

Ausgabe

```
Hello World!
```

Lösung einreichen

Momentan können keine Lösungen eingereicht werden...