Verschlüsseler

Eine einfache symmetrische Verschlüsselung in C#

Grundlagen symmetrische Verschlüsselung

Die Mathematische Operation XOR (Exclusives Oder) funktioniert wie eine Addition auf Bit Ebene.
Das besondere dabei: Bei wiederholter XOR Verknüpfung mit demselben Wert ergibt sich wieder der ursprüngliche Wert.

```
01101110 XOR
10110110 =
11011001
```

```
01101110 XOR
10110110 =
11011001 XOR
10110110 =
01101110
```

Wird nun ein Argument "TextZeichen" und das zweite "SchlüsselZeichen" genannt, so kann das erste Ergebnis "VerschlüsseltesZeichen" genannt werden:

```
TextZeichen XOR
SchlüsselZeichen =
VerschlüsseltesZeichen
```

Ein Text kann prinzipiell verschlüsselt werden, indem jedes TextZeichen mit einem SchlüsselZeichen XOR verknüpft wird. Ist der Schlüssel kürzer als der Text, so wird er mehrfach verwendet.

```
Mein supergeheimer Text
SchluesselSchluesselSch XOR
eCDCRyCFAOyCA7M4yHh2MtM
```

Ein Problem beim Verschlüsseln von lesbaren Texten ist, dass die verwendete ASCII Zeichentabelle viele nicht sichtbare Zeichen und Steuercodes enthält. Wird z.B. irgendein Zeichen mit sich selbst XOR verknüpft, dann ergibt sich immer Null. Die Null ist jedoch nicht sichtbar. Es wäre schwierig einen verschlüsselten Text mit nicht sichtbaren Zeichen an einen Empfänger zu schicken. Eine gängige Lösung ist die Verwendung einer Tabelle mit 64 Zeichen. Diese kann z.B. folgende Zeichen enthalten: a-z, A-Z, 0-9, . (Punkt) sowie ein einfaches Leerzeichen.
Die Zuordnung geschieht in entsprechender Reihenfolge:
0 = 'a', 1 = 'b', ..., 26 = 'A', 27 = 'B', ... 51 = 'Z', 52 = '0', ... 61 = '9', 62 = '.', 63 = ' '

Ein Text aus obigen Zeichen kann dann folgendermaßen in einen verschlüsselten Text aus lesbaren Zeichen überführt (verschlüsselt) werden:
(1) Der Eingabetext wird Zeichen für Zeichen als TextZeichen bearbeitet.
Jedes TextZeichen wird in eine zugehörige TextNummer 0..63 überführt.
(2) Aus dem Schlüssel wird das nächste SchlüsselZeichen entnommen.
Das SchlüsselZeichen wird in eine zugehörige SchlüsselNummer 0..63 überführt.
(3) VerschlüsselteNummer = TextNummer XOR SchlüsselNummer.
(4) Die VerschlüsselteNummer 0..63 wird zurück in ein VerschlüsseltesZeichen überführt.
Das VerschlüsselteZeichen wird an den Verschlüsselten Text angehängt.
(5) Wegen seiner symmetrischen Eigenschaften, liefert die XOR Verknüpfung einer bereits verschlüsselten Nummer mit derselben SchlüsselNummer wieder die TextNummer.
(6) Der letzte Schritt beim Entschlüsseln ist die Rücküberführung der Nummer in ein Zeichen.

(1)	(2)	(3)	(4)	(5)	(6)
M->12	S->18	12 XOR 18 = 30	30->e	30 XOR 18 = 12	12->M
e->30	c->28	30 XOR 28 = 2	2->C	2 XOR 28 = 30	30->e
i->34	h->33	34 XOR 33 = 3	3->D	3 XOR 33 = 34	34->i
n->39	l->37	39 XOR 37 = 2	2->C	2 XOR 37 = 39	39->n
->63	u->46	63 XOR 46 = 17	17->R	17 XOR 46 = 63	63->

Hinweis: In C und C# wird die XOR-Verknüfung durch das Dachsymbol ^ dargestellt.

Aufgabe 1

Schreibe ein Konsolenprogramm, welches in Main()
a) vom Benutzer per Console.ReadLine() erfragt
   String Schluessel = zu verwendendes Schlüsselwort
b) vom Benutzer per Console.ReadLine() erfragt
   String Text = zu verschlüsselnder Text
c) solange b) ausführt bis der Benutzer das Wort „ende“ eingibt.

Aufgabe 2

a) Lade das Modul **Crypto.cs** in das Projektverzeichnis herunter:
   https://halbleiterbauelemente.de/lehre/verschluesseler/
b) Füge das Modul Crypto.cs zum C# Projekt hinzu.

Aufgabe 3

Schreibe eine Methode **String verschluessele_text(String Text, String Schluessel)**
a) welche ein Objekt der Klasse Crypto als MyCrypto instanziiert
b) welche MyCrypto.verschluessle_zeichen() benutzt um jedes einzelne Zeichen von Text mit einem Zeichen von Schluessel verschluesselt.
c) welche alle verschluesselten Zeichen in einem String namens VerschluesselterText sammelt.
d) welche VerschluesselterText zurück gibt

Aufgabe 4

Erweitere Main() so, daß Text und Schluessel mittels verschluessele_text() den kompletten Text verschüsselt und diesen auf der Konsole ausgibt.

Beispielsitzung:

```
********************************
******** Verschlüsseler ********
********************************

Eingabe von ende beendet das Programm.

Schlüsselwort? (123456) = Schluessel
Text = Mein supergeheimer Text
Verschlüsselt = eCDCRyCFAOyCA7M4yHh2MtM

Text = eCDCRyCFAOyCA7M4yHh2MtM
Verschlüsselt = Mein supergeheimer Text

Text = ende
```