Ein einfaches Verschlüsselungsverfahren arbeitet wie folgt: Zeichen werden als Bitfolgen aufgefasst (hier: als Bytes, also Folgen von 8 Bits).

Zeichen	*Byte*		*Zeichen*	*Byte*		*Zeichen*	*Byte*		*Zeichen*	*Byte*
A	*01000001*		*B*	*01000010*		*C*	*01000011*		*D*	*01000100*
E	*01000101*		*F*	*01000110*		*G*	*01000111*		*H*	*01001000*
I	*01001001*		*J*	*01001010*		*K*	*01001011*		*L*	*01001100*
M	*01001101*		*N*	*01001110*		*O*	*01001111*		*P*	*01010000*
Q	*01010001*		*R*	*01010010*		*S*	*01010011*		*T*	*01010100*
U	*01010101*		*V*	*01010110*		*W*	*01010111*		*X*	*01011000*
Y	*01011001*		*Z*	*01011010*						

Zwei Zeichen werden miteinander verschlüsselt, indem man sich die Bitfolgen übereinander hingeschrieben denkt und die jeweils übereinander stehenden Bits XOR-verschlüsselt: sind die Bits gleich, dann ist das Ergebnis eine Null, sonst eine Eins.

Beispiel:

E: *01000101*
X: *01011000*
ergibt: 00011101

Das Verschlüsselungsverfahren soll dann wie folgt arbeiten: Die Zeichen des Klartextes werden zeichenweise mit den Zeichen des Schlüssels xor-verschlüsselt. Ist der Schlüssel kürzer als der Klartext, dann wird bei Bedarf von vorne begonnen.

a: Verschlüsseln Sie „per Hand" das Wort „AFFE" mit dem Schlüssel „DU".

b: Vergleichen Sie das Vigenere-Verfahren mit der XOR-Verschlüsselung.

c: Wie können XOR-verschlüsselte Texte wieder entschlüsselt werden?