Solution of Exercisesheet 2

Exercise 2-1

If the one-time pad could be used twice with the same key and achieve perfect security, the following equation would be true:
$Pr[M_1 = m_1 \wedge M_2 = m_2 | C_1 = c_1 \wedge C_2 = c_2] = Pr[M_1 = m_1 \wedge M_2 = m_2]$

Let $c_1 = c_2, m_1 \neq m_2$
Then $Pr[M_1 = m_1 \wedge M_2 = m_2 | C_1 = c_1 \wedge C_2 = c_2] = 0$ due to the correctness.
But $Pr[M_1 = m_1 \wedge M_2 = m_2] = Pr[M_1 = m_1]Pr[M_2 = m_2] \neq 0$
therefore
$Pr[M_1 = m_1 \wedge M_2 = m_2 | C_1 = c_1 \wedge C_2 = c_2] \neq Pr[M_1 = m_1 \wedge M_2 = m_2]$ $\square$

Solution of Exercisesheet 2

Exercise 2-2

Decoded message:
ONE MUST ACKNOWLEDGE WITH CRYPTOGRAPHY NO AMOUNT OF VIOLENCE WILL EVER SOLVE A MATH PROBLEM

Using the XOR of both messages we can decode the second message if we know the first.
$c1 \oplus c2 = (k \oplus m1) \oplus (k \oplus m2) = (k \oplus k) \oplus (m1 \oplus m2) = m1 \oplus m2$

Since we know one message starts with "ONE MUST " and contains " WITH " we get the start of the other message "OF VIOLEN" by reversing the XOR operation:
$(c1 \oplus c2) \oplus m1 = (m1 \oplus m2) \oplus m2 = m1 \oplus (m2 \oplus m2) = m2$
By guessing further letters from the context and finding the word " WITH " in one message we can decode the rest of the sentence.

Solution of Exercisesheet 2

Exercise 2-3

f and g are negligible functions and q be a positive polynomial.

(a) Is e^{-x} negligible?
For any polynomial x^c, choose $N = c$, then for all $x > N$ holds:
$e^{-x} < \frac{1}{x^c}$, because $e^x > x^c$ for all $x > N = c$.
$\Rightarrow e^{-x}$ is negligible.

(b) Is $\frac{1}{x^{2021}+1}$ negligible?
For the polynomial x^{2022} there is no N, that for all $x > N$ holds:
$\frac{1}{x^{2021}+1} < \frac{1}{x^{2022}}$, because $x^{2021} + 1$ is smaller than x^{2022} for $x > 1$.
$\Rightarrow \frac{1}{x^{2021}+1}$ is not negligible.

(c) Is $h(x)$ negligible, when $h(x)$ is a positive function such that $h(x) < f(x)$ for all x?
For $f(x)$ holds: $f(x) < \frac{1}{p(x)}$ (Definition 0.1).
Because of $h(x) < f(x) < \frac{1}{p(x)}$ for all x, $h(x)$ is also negligible.

(d) Is $f(x) + g(x)$ negligible?
$f(x)$ negligible $\Rightarrow f(x) < \frac{1}{p(x)}$ (Definition 0.1).
$g(x)$ negligible $\Rightarrow g(x) < \frac{1}{p'(x)}$ (Definition 0.1).

$$\begin{aligned}\Rightarrow f(x) + g(x) &< \frac{1}{p(x)} + \frac{1}{p'(x)} \\ &= \frac{p'(x) + p(x)}{p(x) \cdot p'(x)} \\ &= \frac{1}{\frac{p(x)\cdot p'(x)}{p'(x)+p(x)}}\end{aligned}$$

Addition, multiplication and division of two polynomials results in another polynomial. $p(x)$ and $p'(x)$ can be any polynomials. Because of that the denominator ($\frac{p(x)\cdot p'(x)}{p'(x)+p(x)}$) can also be any polynomial.
$\Rightarrow f(x) + g(x)$ is negligible.

(e) Is $f(x) \cdot q(x)$ negligible?
$f(x)$ negligible $\Rightarrow f(x) < \frac{1}{p(x)}$ (Definition 0.1).
$q(x)$ is a positive polynomial.

$$\begin{aligned}\Rightarrow f(x) &< \frac{1}{p(x)} \qquad | \cdot q(x), q(x) positive \\ f(x) \cdot q(x) &< \frac{q(x)}{p(x)} \\ f(x) \cdot q(x) &< \frac{1}{\frac{p(x)}{q(x)}}\end{aligned}$$

Solution of Exercisesheet 2

Division of two polynomials results in another polynomial. $p(x)$ can be any polynomial. So the denominator ($\frac{p(x)}{q(x)}$) can also be any polynomial.
$\Rightarrow f(x) \cdot q(x)$ is negligible.

(f) Is $\frac{f(x)}{g(x)}$ negligible?
$f(x)$ negligible $\Rightarrow f(x) < \frac{1}{p(x)}$ (Definition 0.1).
$g(x)$ negligible $\Rightarrow g(x) < \frac{1}{p'(x)}$ (Definition 0.1).

$$\Rightarrow \frac{f(x)}{g(x)} < \frac{\frac{1}{p(x)}}{\frac{1}{p'(x)}}$$
$$\frac{f(x)}{g(x)} < \frac{1}{\frac{p(x)}{p'(x)}}$$

Division of two polynomials results in another polynomial. $p(x)$ and $p'(x)$can be any polynomials. So the denominator ($\frac{p(x)}{p'(x)}$) can also be any polynomial.
$\Rightarrow \frac{f(x)}{g(x)}$ is negligible.

(g) Is $2^{-1024} = \frac{1}{2^{1024}}$ negligible?
For the polynomial x^{1025} there is no N, that for all $x > N$ holds:
$\frac{1}{2^{1024}} < \frac{1}{x^{1025}}$, because 2^{1024} is always smaller than x^{1025} for all $x > 1$.
$\Rightarrow 2^{-1024}$ is not negligible.

(h) Is $(f(x))^{\frac{1}{q(x)}}$ negligible?
$f(x) = e^{-x}$ is negligible (see (a))
$q(x) = x$ is a positive polynomial for all $x > 0$
$\Rightarrow (e^{-x})^{\frac{1}{x}} = e^{-1} = \frac{1}{e}$
For the polynomial x^2 there is no N, that for all $x > N$ holds:
$\frac{1}{e} < \frac{1}{x^2}$, because e is always smaller than x^2 for all $x \geq 2$.
$\Rightarrow e^{-1}$ is not negligible. $\Rightarrow (f(x))^{\frac{1}{q(x)}}$ is not negligible.

(i) Is $x^{-\log\log\log x}$ negligible?
For any polynomial x^c, choose $N = e^{e^{e^c}}$, then for all $x > N$ holds:
$x^{-\log\log\log x} < \frac{1}{x^c}$, because $x^{\log\log\log x} > x^c$ and $\log\log\log x > c$ for all $x > N = e^{e^{e^c}}$.
$\Rightarrow x^{-\log\log\log x}$ is negligible.

Solution of Exercisesheet 2

Exercise 2-4

In this experiment the adversary A recieves a random message m* with its encryption c* from the challenger using the secret key (a, b). Adversary A now generates two messages m_0 and m_1 of the same length that must be distinct from m*.
Our challenger chooses one of them and encrypts them using the encryption scheme: $c = a \cdot m_b + b$

To crack the encryption the adversary A has information about c*, m* and c.
That means adversary A has to solve these equations:
$c^* = a \cdot m^* + b$
$c = a \cdot m_b + b$
to get the secret key (a,b).
However since A is missing the information about m_b the system of equations is over-determined and not solvable.
This means A has to guess which message was encrypted and
Pr [TTP - SEC $= 1] = \frac{1}{2}$

Solution of Exercisesheet 2

Exercise 2-5

(a) For the case when length of message, l_m, is greater than length of key, l_k ie., $l_m > l_k$

Some parts of the message are encrypted with the same key. It is like using one time pad multiple times with same key.

As mention in page 36 of [1], *"the one-time pad scheme — as the name indicates — is only 'secure' if used once (with the same key). ..... it is easy to see informally that encrypting more than one message leaks a lot of information. In particular, say two messages are encrypted using the same key k. and thus learn something about the exclusive-or of the two messages. While this may not seem very significant, it is enough to rule out any claims of perfect secrecy when encrypting two messages. Furthermore, if the messages correspond to English language text, then given the exclusive-or of sufficiently many message pairs it is possible to perform frequency analysis .... and recover the messages themselves"*

Hence this scheme is not perfectly secure for $l_m > l_k$

(b) This encryption scheme can be made secure by atleast restricing the length of key as close as length of message. such that $(l_m - l_k)$ is almost close to zero or (l_k/l_m) is almost approximated to 1.

or contacting different keys in such a way $l_k > l_m$

References

[1] Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography (2nd ed.). Chapman and Hall/CRC. https://doi.org/10.1201/b17668