

Exercises for the lecture
Cryptography

Exercise Sheet 3
for the exercise on November 6th, 2026

Exercise 3.1

Decrypt.

(will not be done during exercise)

CfwnjhyvdlfsfxxJuxpqsjyaqqxjQcuazhxtqpSdrylafSfftxzukmaktwnkuz
kqkywgNlsfhfguakgkbjEsaeojzniAsagkCgnxbftbtgkgsfsvxxZglzfsEhj
hymnbbyzkwkbhq0dekPkgozvbwgchxwakPjnk gkSlrwbvtvggbqsjYrxkzaikw
brwCxiasjzxrylaTijymhrnjdsfXoqklBosmgjhyYnbifwfyxekKwkkltaki
rwlChouaofmgmhtFepqzxyhogakXmukokbjGooxxdavidkijxoqkLabzwLkltg
akbltaijxiBfvxtuagzRbvpkuygebuwduqtmzbfkmkkrxSbwfxtgybyeomlj1
klajPmgjIxxqaslkoqqxjzdxChyxjXbvxtExnaphwgjhxGwqijTrokZqqsft
rokUkbgwgLrrzakwzkkuXhobbkiaUQnapgwzgeybarbkntgXxxbbWbthtYnbi
fwmhvkqbtlbsWuwSlzdneywctnarwfCxxfcuwukqagzasjVnhxnxphwazyukC
lhlYxrnpebgwbthYhksfyrllkzakRmkikjxoEwefkoyinxsuazlmxjMzsgRda
yaqPjnk gkkarfwUgktYnbivbmzoxafbZxrgfniPwwzkqYxeaielikrnjdsfFo
orbkksfWohyxjHikljhxzwknwgChrmXoiwwkuaxxbfeLzhxgknwezPalobwf
eohhxnSolxxzuajbbAaxvznaonlgohjxnJwdeortxjXvfywjnzbbKvnrkibb
f0xrwYnyewzgahhxnjGlxxqkgvbzlNkekk0qsjgkqsnopsjpuktxj

(Ciphertext available in Moodle; capitalization only for readability; lower- and upper-case letters can be treated the same)

Exercise 3.2

Are ciphertexts uniformly distributed in a perfectly secret encryption scheme?

Prove or refute: Given a perfectly secret encryption scheme $\mathcal{E}$ with message space M and ciphertext space C and an arbitrary scenario $(\mathcal{E}, P_M)$, we have $P(c) = P(c')$ for all ciphertexts $c, c' \in C$.

Exercise 3.3

Prove that decryption can always be derandomized in every encryption scheme $\mathcal{E}$. Formally, given encryption scheme $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ with $\text{dec}: R \times K \times C \rightarrow M$, prove

that $\text{dec}(r, k, c) = \text{dec}(r', k, c)$ for all $r, r' \in R$, every possible key $k \in \text{ran}(\text{gen})$, and every suitable ciphertext $c \in C$; i.e., there exists $m \in M$ such that $P[c \leftarrow \text{enc}_k(m)] \neq 0$. In other words, decryption does not depend on the random bit tape. Mind that $\mathcal{E}$ need not be perfectly secret.

Exercise 3.4

Is one-time pad still perfectly secret if multiple messages are encrypted with the same key? Justify your answer, so either prove or refute perfect secrecy. If it is not perfectly secret, then also answer whether realistic attacks are possible and outline how you would proceed to break such a cipher.