Model 8: Encryption

Objectives and classification

Overview
After the introduction to message transmission in Model 7, this model deals with the protection of transmission by encryption. Two simple encryption methods introduce the functionality of a substitution cipher and the concept of key-controlled encryption.

Topics
How can data transmission be protected from „eavesdroppers"? How does encryption work? What is a „key"?

Learning objectives

- Encryption as protection against „eavesdropping"
- Principle of the „shared secret"
- Principle of a key-based cipher
- Programming an encrypted transmission
- Determination of the „key space" of a cipher
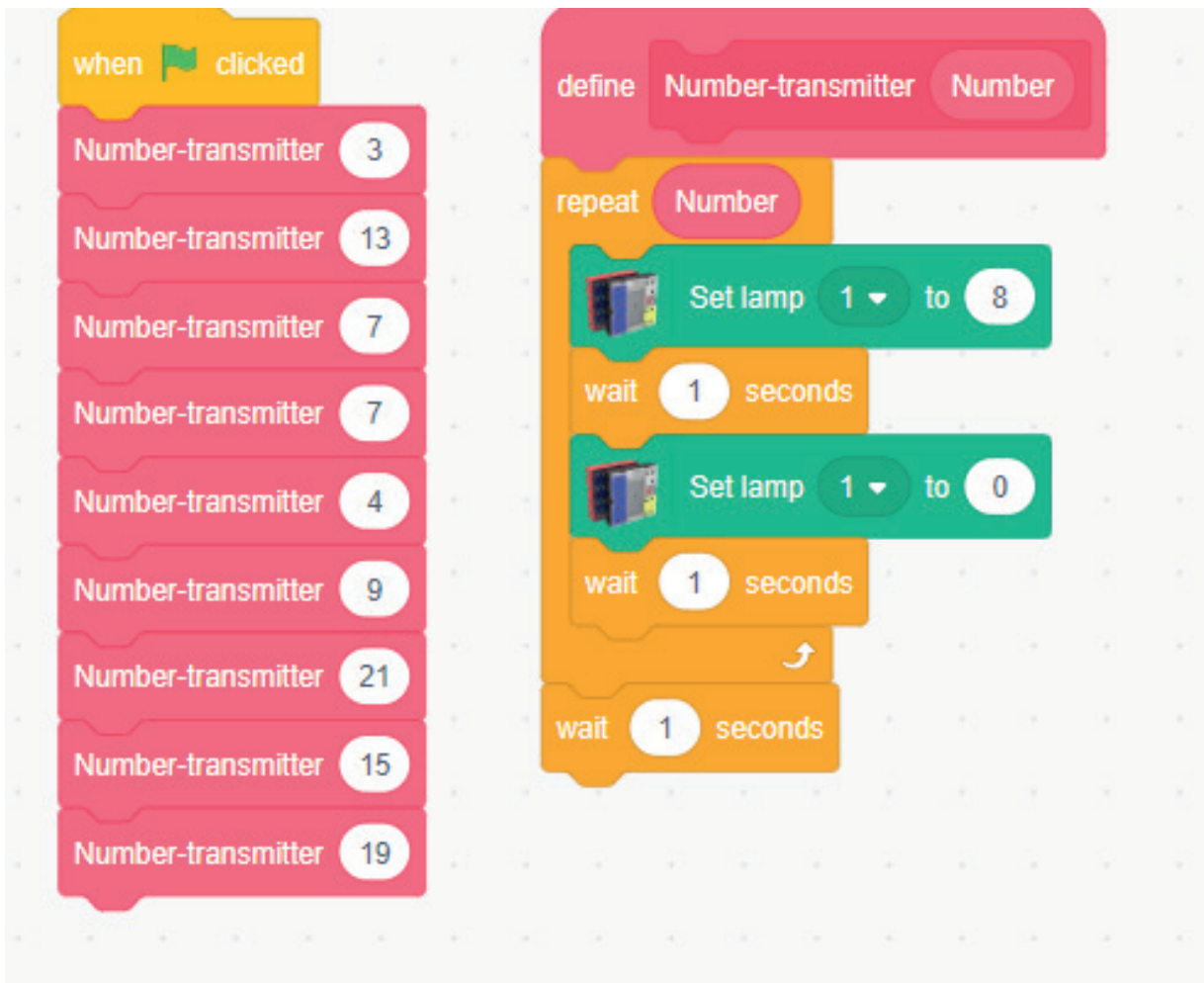
Time required
The „Encryption" model is developed using two separate building instructions for the Receiver model and the Transmitter model. Please pay attention to both tasks and let the teams build one model each.
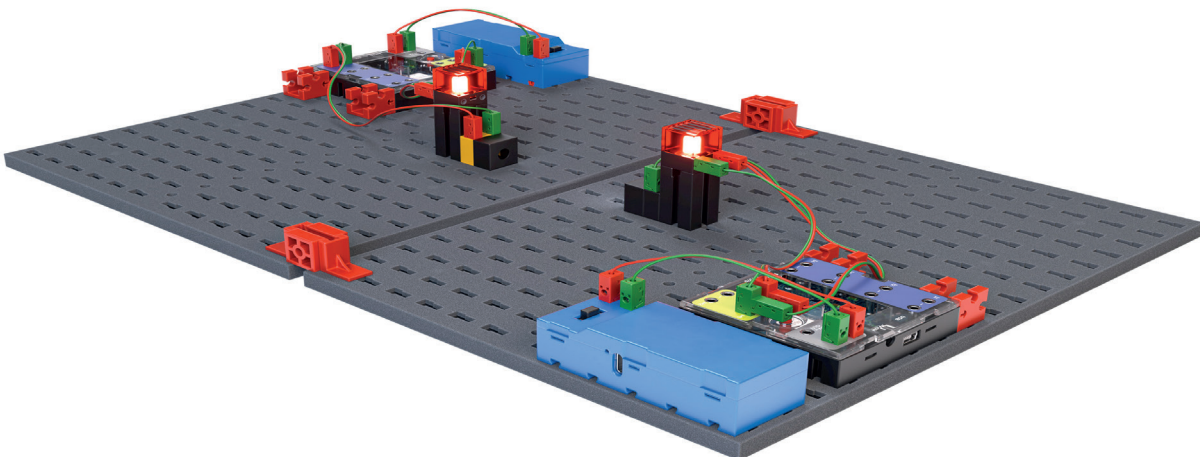
Solutions and notes
Programming tasks Model 8: Encryption

Solution:

Message encrypted sender.sb3

A		G		M		S		Y	
B		H	**13**	N		T		Z	
C		I		O	**13**	U			
D	**13**	J		P		V			
E	**13**	K		Q		W	**13**		
F		L	**13**	R	**13**	X			

Solutions and notes
Programming tasks Model 8: Encryption
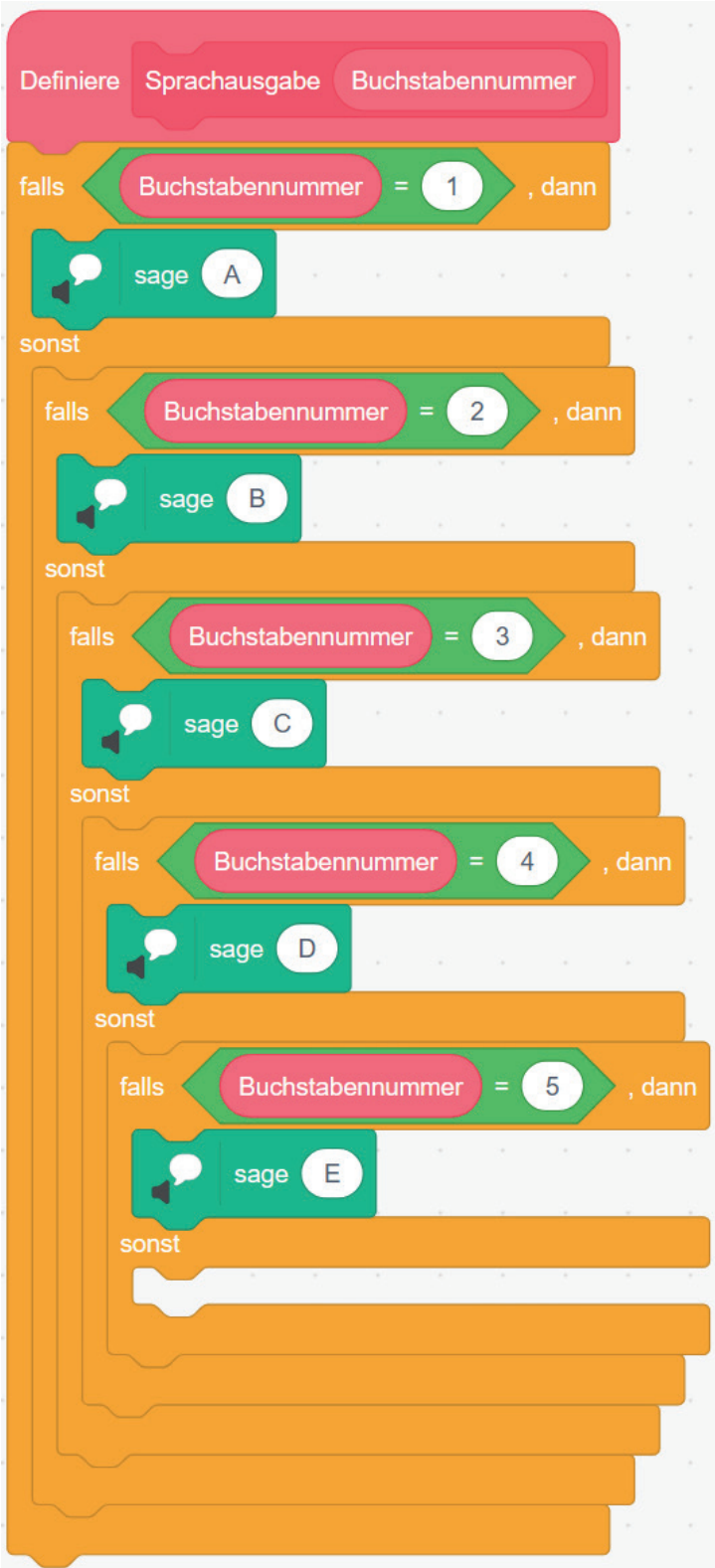
Solution:

Message encrypted recipient.sb3

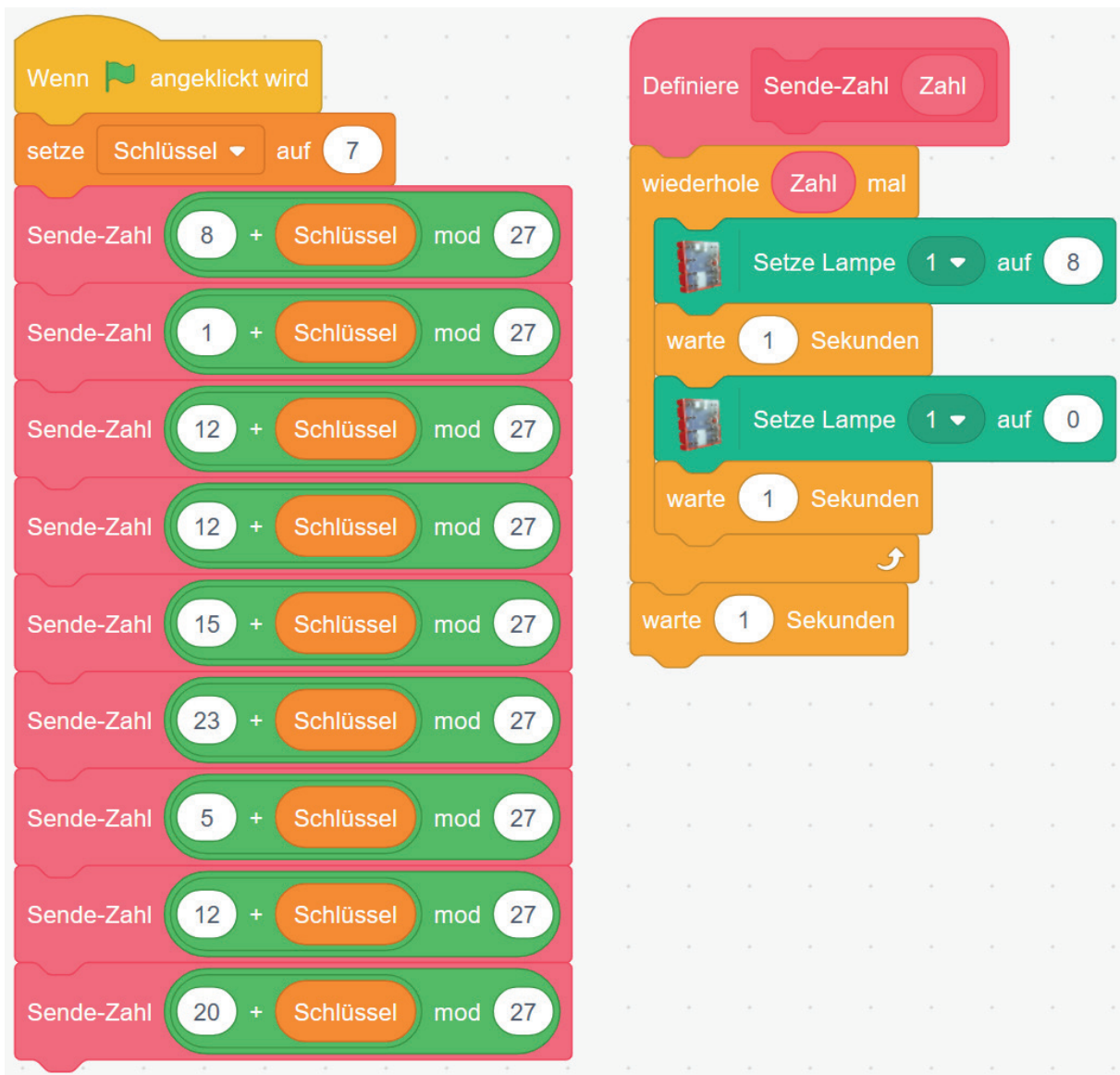# Solutions and notes
Programming tasks Model 8: Encryption

Message postponed sender.sb3

Solutions and notes
Programming tasks Model 8: Encryption
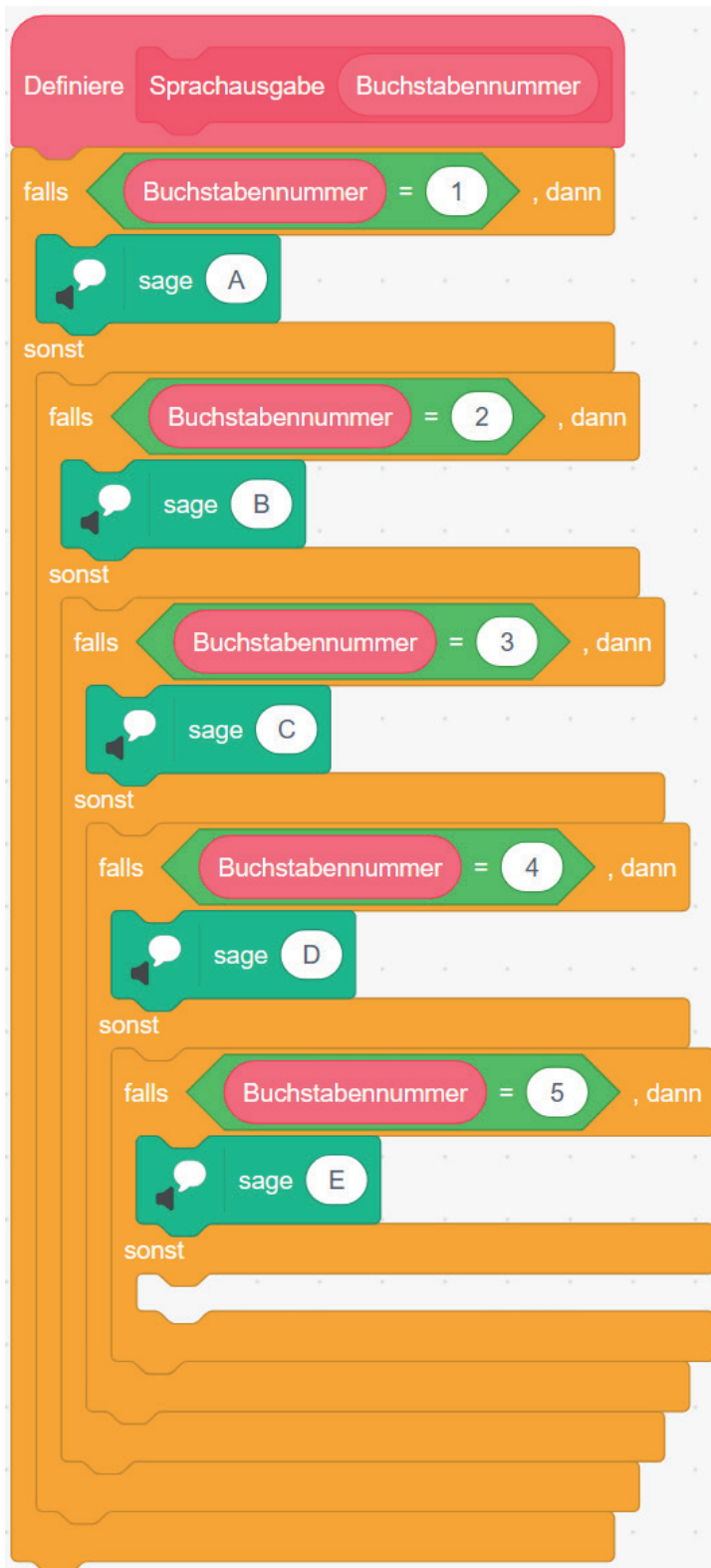
Solution:

Message postponed recipient.sb3

Solutions and notes
Programming tasks Model 8: Encryption

Suggested solution Task Voice output - extract subroutine:

Voice output receiver with encryption.sb3