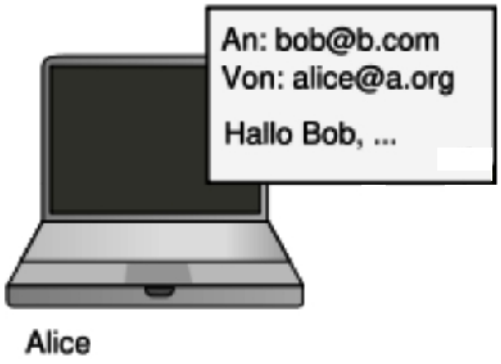
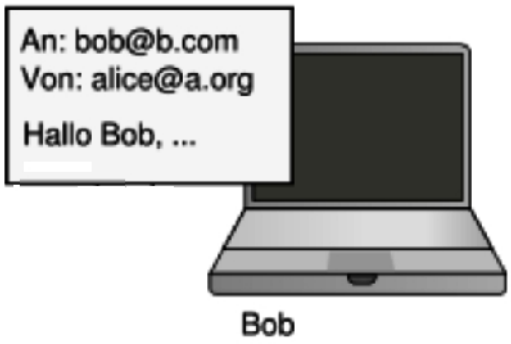
Informatik **Datum:**
Prüfziffern Datei:06_Münzwurf-Email.odt **Name:**

Per E-Mail eine Münze werfen





Können Alice und Bob ihre Entscheidung (den Münzwurf) auch per Mail abwickeln?

Alice überlegt: Wenn ich die Worte "Alice" und "Bob" mit einer Einwegfunktion kodiere und die Ergebnisse an Bob schicke, dann kann er ganz einfach herausfinden, welche Zahl zum Wort "Alice" und welche zum Wort "Bob" gehört. Ich muss also "etwas" in das Verfahren hineinbringen, dass ich erst später an Bob verrate.

Alice schlägt vor:
"Ich denke mir zwei beliebige Buchstaben aus und hänge daran "al". An zwei andere frei wählbare Buchstaben hänge ich "bo". Diese beiden vier Buchstaben langen Wörter kodiere ich mit der bekannten Einwegfunktion und schicke diese beiden entstehenden Zahlen an Dich. Du "ziehst" dann eine der Zahlen und teilst mir deine Wahl mit. Daraufhin schicke ich Dir die beiden ursprünglichen Wörter. Du kannst prüfen, welches Wort zu der gewählten Zahl gehört und an den beiden letzten Buchstaben erkennen, wer gewonnen hat."

Alice		**Bob**
Alice bildet: bo -> kobo -> 5516 al -> sial -> 7625	→	Alice schreibt: "Zur Wahl stehen die Zahlen 5516 und 7625"
Bob schreibt: „Ich habe die Zahl 7625 gewählt"	→	Alice schreibt: "Die Zahl 7625 steht für **sial**, also habe ich gewonnen. 5516 stand für **kobo**. Du kannst es prüfen"

Bob ist mit dem Vorschlag von Alice einverstanden. Doch nach einiger Zeit wird er misstrauisch: Immer gewinnt Alice! kann Sie schummeln, oder hat sie nur Glück?

kobo, sial, bual, opbo