Sporočila ne kodiramo le zato, da jih je možno poslati po določenem mediju, ampak tudi zato, da bi jih ne prebral (in zlorabil) kdorkoli.

Kriptologija je veda o tajnosti, šifriranju, zakrivanju sporočil (kriptografija) in o razkrivanju šifriranih podatkov (kriptoanaliza).

Sporočilo po nekem postopku (algoritmu, metodi) spremenimo v kriptirano sporočilo: tajnopis, pri tem uporabimo določene vrednosti za parametre v algoritmu, ki jim rečemoključ. Sogovornika se morata dogovoriti o algoritmu in ključu, da si lahko pošiljata šifrirana sporočila.

Jana in Miha sta se sporazumela, da si bosta svoj »tajnopis« izmenjevala tako, da si bosta na v naprej določenem skritem mestu pustila ključ (varni kanal), po katerem bosta s pomočjo spodnje matrike zakriptirala svoja sporočila.

Primer kriptiranja sporočila, ki ga je sporočila Jana Mihu: **Jutri ob osmih pri starem hrastu**.
Za ključ: **šifriranje:**

Ključ: Š I F R I R A N J E Š I F R I R A N J E Š

Čistopis: J U T R I O B O S M I H P R I H R A S T U

Tajnopis:D E B I S G B D Č S Č R V I S A R N Č A O

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 |  | A | B | C | Č | D | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž |
| 1 |  | B | C | Č | D | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž | A |
| 2 |  | C | Č | D | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž | A | B |
| 3 |  | Č | D | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž | A | B | C |
| 4 |  | D | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž | A | B | C | Č |
| 5 |  | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž | A | B | C | Č | D |
| 6 |  | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž | A | B | C | Č | D | E |
| 7 |  | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž | A | B | C | Č | D | E | F |
| 8 |  | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž | A | B | C | Č | D | E | F | G |
| 9 |  | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž | A | B | C | Č | D | E | F | G | H |
| 10 |  | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž | A | B | C | Č | D | E | F | G | H | I |
| 11 |  | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž | A | B | C | Č | D | E | F | G | H | I | J |
| 12 |  | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž | A | B | C | Č | D | E | F | G | H | I | J | K |
| 13 |  | M | N | O | P | R | S | Š | T | U | V | Z | Ž | A | B | C | Č | D | E | F | G | H | I | J | K | L |
| 14 |  | N | O | P | R | S | Š | T | U | V | Z | Ž | A | B | C | Č | D | E | F | G | H | I | J | K | L | M |
| 15 |  | O | P | R | S | Š | T | U | V | Z | Ž | A | B | C | Č | D | E | F | G | H | I | J | K | L | M | N |
| 16 |  | P | R | S | Š | T | U | V | Z | Ž | A | B | C | Č | D | E | F | G | H | I | J | K | L | M | N | O |
| 17 |  | R | S | Š | T | U | V | Z | Ž | A | B | C | Č | D | E | F | G | H | I | J | K | L | M | N | O | P |
| 18 |  | S | Š | T | U | V | Z | Ž | A | B | C | Č | D | E | F | G | H | I | J | K | L | M | N | O | P | R |
| 19 |  | Š | T | U | V | Z | Ž | A | B | C | Č | D | E | F | G | H | I | J | K | L | M | N | O | P | R | S |
| 20 |  | T | U | V | Z | Ž | A | B | C | Č | D | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š |
| 21 |  | U | V | Z | Ž | A | B | C | Č | D | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T |
| 22 |  | V | Z | Ž | A | B | C | Č | D | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U |
| 23 |  | Z | Ž | A | B | C | Č | D | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V |
| 24 |  | Ž | A | B | C | Č | D | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z |
| 25 |  | A | B | C | Č | D | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. Kaj je Miha sporočil Jani s tajnopisom JBOUNE**,** ko je uporabil isti ključ? (2 točki)

2. Kateri ključ pa je uporabila Jana, ko je po enakem postopku za čistopis: »DANES NE PRIDEM**«** poslala tajnopis: » OOSEDDIPČŽHEŽ«? (2 točki)

3. Kaj je osnovni problem, nastopa pri kodiranju, kjer se uporablja isti ključ za kodiranje in dekodiranje sporočila? (1 točka)

Rešitev:

1. Mija je sporočil Jani: PRIDEM

2. Nov ključ je: KODA

3. Kako omogočiti »varni kanal«.