

HW1 of Introduction to Information Security 2018

Plaintext: keepgoingnevergiveup

1. Caesar cipher:

key: 7

2. Monoalphabetic cipher:

key:

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | |
| | | | | | | | | | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 |
| z | y | x | w | v | u | t | s | r | q | p | o | n | m | l | k | j | i | h | g | f | e | d | c | b | a |
| M | N | B | V | C | X | Z | L | K | J | H | G | F | D | S | A | P | O | I | U | Y | T | R | E | W | Q |

3. Playfair cipher:

key: HIT

4. Vernam proposed the autokey system

key: CON

5. Row transposition:

key: 31562487

6. Product cipher:

Key:

| | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|
| 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

Transport:

| | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|
| 15 | 11 | 19 | 18 | 16 | 03 | 07 | 14 | 02 | 20 |
| 04 | 12 | 09 | 06 | 01 | 05 | 17 | 13 | 10 | 08 |