Cryptography vs. Coding theory

Protecting communication over noisy channel

Alice - Bob - Eve

Alice - plaintext Encrypt Cipher text Decrypt Bob

Eve knows this code, and ciphertext
Enc key Eve dec key

Mallory (alter the message, pretend to be Alice)

Possible attacks:

* Kerckhoff’s principle: Eve knows the encryption method.
  - Ciphertext only.
  - Known plaintext. (Dear Bob, Sahara Desert)
  - Chosen plaintext. (Eve get temporary access to the encryption code)
  - Chosen ciphertext (.... dec code)

Shift cipher:
- a...z → 0...25. (omit spaces and punctuations)
- enc. key is an integer \( k \): \( 0 \leq k \leq 25 \).
- \( m \): Cat \( \rightarrow \frac{k=2}{ECV} \) : C
- encryption: \( c = (m + k) \mod 26 \).
- decryption: \( m = (c - k) \mod 26 \).

Attacking Shift cipher:
- ciphertext only. (try \( k = 0...25 \))
- known plaintext: \( (a, c) \rightarrow k=2 \).
- chosen plaintext: choose “a”.
- chosen ciphertext: choose “A”.