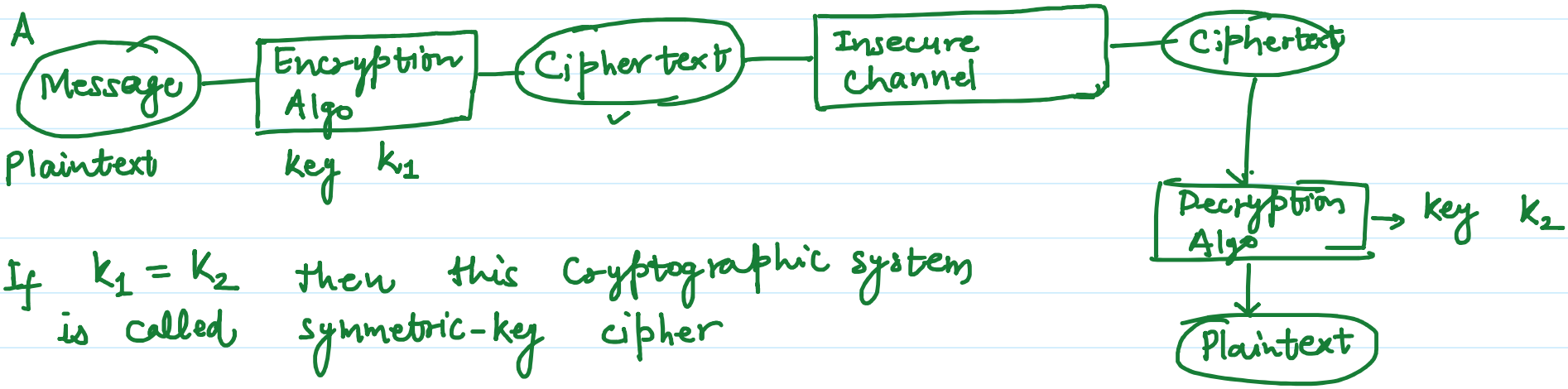
Security Goals:

1. Confidentiality
2. Integrity
3. Availability

Crypto + Graphy
- Secret Writing.



If $k_1 = k_2$ then this cryptographic system is called symmetric-key cipher

If $k_1 \neq k_2$ then this cryptosystem is called Asymmetric-key cipher.

Symmetric key Cipher.

$E_k(P)$ — Encryption Algo
(k ↓ plaintext)

$D_k(C)$ — Decryption Algo.
(k ↓ Ciphertext)

$E_k(P) = C$: Encryption

$D_k(C) = P$: Decryption

$$D_K(E_K(x)) = x = E_K(D_K(x))$$

11 August 2020 09:18

Kerckhoff's Principle: Guessing the key should be so difficult that there is no need to hide the encryption/decryption algorithm.

Cryptanalysis: Science or art of breaking ciphers.

Cryptanalysis Attacks:

(1) Ciphertext Only: Eve (Adversary) has the access to some ciphertext and it is assumed that Eve knows the encryption/dec. algorithm.

(i) Brute Force (or exhaustive-key attack): to prevent it, key domain should be very large.

(ii) Statistical Attack: Eve can use some inherit characterstics of the plaintext language.

To prevent this attack, cipher should hide the characterstics of the plaintext language

(iii) Pattern Attack : There should not be any pattern in the ciphertext.

2. known-Plaintext Attack: Eve has the access to some P/C pair in addition to the intercepted ciphertext.

⇒ less likely to happen

→ Ciphertext only attacks can also be applied here.

→ Easier to implement.

3. Chosen - Plaintext Attack: Eve has the access to Alice's computer then she can choose some plaintext and intercept the created ciphertext.

4. Chosen - Ciphertext Attack: Eve has the access to Bob's computer

Traditional Ciphers

11 August 2020 09:41

(1) Substitution Cipher (2) Transposition Ciphers.

Substitution Ciphers : It replaces one symbol with another.

Ex : hi (plaintext) — KT

[h → K, i → T, ⋮ ⋮] — key

Types :

(i) Monoalphabetic Cipher (ii) Polyalphabetic Cipher.

(i) Monoalphabetic Cipher : Relationship b/w a symbol in the plaintext to a symbol in the ciphertext is one-to-one.

a	b	c	d	e	----
K	L	M	N	O	---.

} key

(ii) Polyalphabetic Cipher : Each occurence of a character may have a different substitute.

Relationship b/w a char. in plaintext to a char. in ciphertext is one-to-many. Ex: Autokey, playfair, vigenere.

Additive Cipher (Ceaser Cipher or Shift Cipher)

11 August 2020 09:51

plaintext	a	b	c	d	e	----
Ciphertext	A	B	C	D	E	---.
value	0	1	2	3	4	---..

$\{0, 1, 2, 3, \text{---}\} = \mathbb{Z}_{26}$

$(\mathbb{Z}_{26}, +_{26})$ – Group.

plaintext : P Ciphertext : C key : k

Encryption : $(P + k) \bmod 26 = C$

Decryption : $(C + (-k)) \bmod 26 = P$

($-k$: inverse of k)

→ Size of the key domain is very small.

26 – keys. $|25|$ – Size of the key domain.

26 — keys. 25 — Size of the key domain.

→ Brute-Force attack can be used very easily.