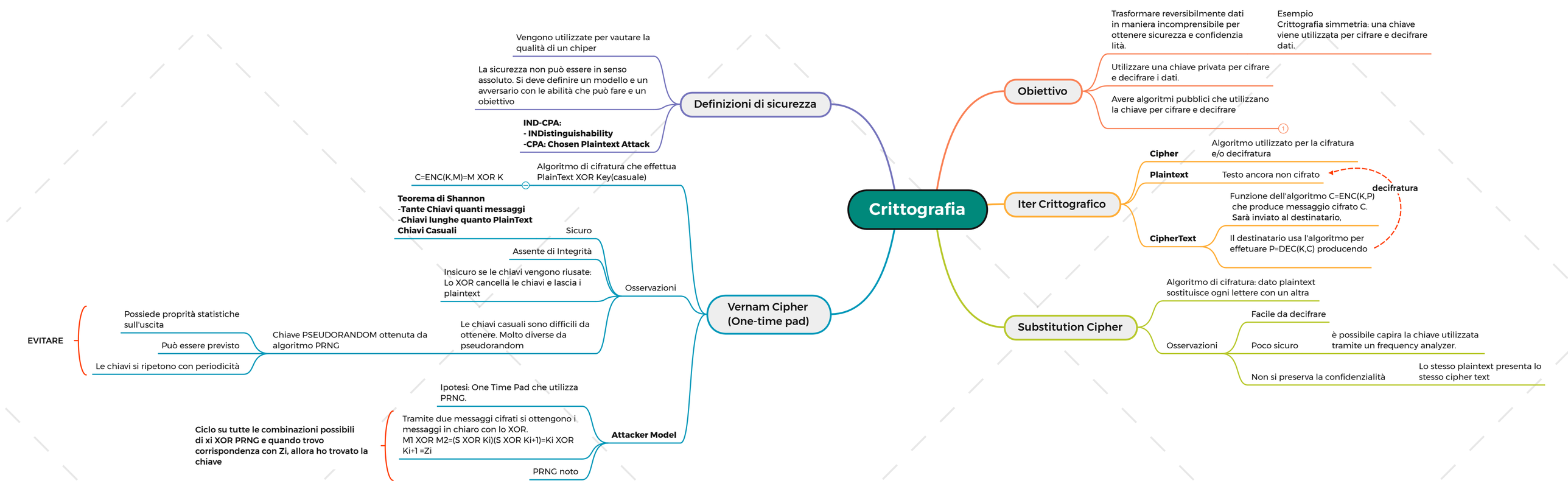
Crittografia
Obiettivo
Trasformare reversibilmente dati in maniera incomprensibile per ottenere sicurezza e confidenzialità.
Esempio
Crittografia simmetria: una chiave viene utilizzata per cifrare e decifrare dati.
Utilizzare una chiave privata per cifrare e decifrare i dati.
Avere algoritmi pubblici che utilizzano la chiave per cifrare e decifrare
Iter Crittografico
Cipher
Algoritmo utilizzato per la cifratura e/o decifratura
Plaintext
Testo ancora non cifrato
decifratura
Funzione dell'algoritmo C=ENC(K,P) che produce messaggio cifrato C. Sarà inviato al destinatario,
CipherText
Il destinatario usa l'algoritmo per effettuare P=DEC(K,C) producendo
Substitution Cipher
Algoritmo di cifratura: dato plaintext sostituisce ogni lettere con un altra
Osservazioni
Facile da decifrare
Poco sicuro
è possibile capira la chiave utilizzata tramite un frequency analyzer.
Non si preserva la confidenzialità
Lo stesso plaintext presenta lo stesso cipher text
Definizioni di sicurezza
Vengono utilizzate per vautare la qualità di un chiper
La sicurezza non può essere in senso assoluto. Si deve definire un modello e un avversario con le abilità che può fare e un obiettivo
IND-CPA:
- INDistinguishability
-CPA: Chosen Plaintext Attack
Vernam Cipher (One-time pad)
Algoritmo di cifratura che effettua PlainText XOR Key(casuale)
C=ENC(K,M)=M XOR K
Teorema di Shannon
-Tante Chiavi quanti messaggi
-Chiavi lunghe quanto PlainText
Chiavi Casuali
Osservazioni
Sicuro
Assente di Integrità
Insicuro se le chiavi vengono riusate: Lo XOR cancella le chiavi e lascia i plaintext
Le chiavi casuali sono difficili da ottenere. Molto diverse da pseudorandom
Chiave PSEUDORANDOM ottenuta da algoritmo PRNG
EVITARE
Possiede proprità statistiche sull'uscita
Può essere previsto
Le chiavi si ripetono con periodicità
Attacker Model
Ipotesi: One Time Pad che utilizza PRNG.
Tramite due messaggi cifrati si ottengono i messaggi in chiaro con lo XOR.
M1 XOR M2=(S XOR Ki)(S XOR Ki+1)=Ki XOR Ki+1 =Zi
Ciclo su tutte le combinazioni possibili di xi XOR PRNG e quando trovo corrispondenza con Zi, allora ho trovato la chiave
PRNG noto