1) modelul COA (cipher text only attack)

=) atacatorul vede criptotextul și vrea să deducă mesajul sau cheia -

2) KPA (known plain text attack)

-> adversarul de-a lungul timpului a știut tot că $m_1$ a fost criptat prin $c_1$

$m_e$ a fost criptat prin $c_e$

-> încearcă să găsească mesajul sau cheia.

Modele active

1) CPA -(choosen plaintext attack)

-> adversarul are posibilitatea să obțină criptotextul asociat unui plaintext ales de el (inductive attack)

2) CCA - choosen ciphertext attack -

adversarul are posibilitatea de a afla mesajele originale asociate unor criptotexte (poate fi făcut și adaptiv => adv. își poate alege el un criptotext și să întrebe care e mesajul original corespunzător)

- CCA e cel mai puternic (primitivă ca să fie rezistentă la CCA)

Și tehnici prin care scheme de criptare la atacuri CPA pot fi transformate în scheme CCA sigure.