Cryptography and Architectures for Computer Security - Cheat Sheet

Information Theory

$Pr(C = c) = \sum_{k:c \in \{\mathbb{E}_k(m), \forall m \in \mathcal{M}\}} Pr(K = k) Pr(P = \mathbb{D}_k(c))$
Perfect secrecy: $Pr(P = m|C = c) = Pr(P = m) \implies |\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$
Entropy: $H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i \quad (p_i \log_2 p_i = 0 \text{ for } p_i = 0)$
$H(X, Y) = -\sum_{i=1}^{n} \sum_{j=1}^{m} Pr(X = x_i, Y = y_j) \log_2 Pr(X = x_i, Y = y_j)$
$H(X|Y = y) = -\sum_{i=1}^{n} \sum_{j=1}^{m} Pr(X = x_i|Y = y) \log_2 Pr(X = x_i|Y = y)$
$H(X|Y) = -\sum_{i=1}^{n} \sum_{j=1}^{m} Pr(Y = y_j) Pr(X = x_i, Y = y_j) \log_2 Pr(X = x_i|Y = y_j)$
$H(X) + H(Y) \geqslant H(X, Y)$; $H(X, Y) = H(Y) + H(X|Y)$; $H(X|Y) \leqslant H(X)$
Key equivocation: $H(K|C) = H(P) + H(K) - H(C)$
Language redundancy: $R_L = 1 - \frac{H_L}{\log_2 |\mathcal{M}|}$
Spurious keys: $\bar{s_n} \geqslant \frac{|\mathcal{K}|}{|\mathcal{M}|^{nR_L}} - 1$
Unicity distance: $n_0 \approx \frac{\log_2 |\mathcal{K}|}{R_L \log_2 |\mathcal{M}|}$

Symmetric Ciphers

Hash Functions

Algebraic Structures

Elliptic Curves

Public Key Cryptosystems

Montgomery Multiplication

Number Theoretical Cryptanalysis

Misc