

Cryptography and Architectures for Computer Security - Cheat Sheet

Information Theory

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

Symmetric Ciphers

Modes of Operation

$$\begin{aligned} \text{ECB: } c_i &= \mathbb{E}_k(m_i) \\ \text{CBC: } c_0 &= IV, c_i = \mathbb{E}_k(m_i \oplus c_{i-1}) \\ \text{CFB/OFB: } ISR_0 &= IV, OSR_i = \mathbb{E}_k(ISR_{i-1}), c_i = m_i \oplus \text{j-th leftmost bits of } OSR_i \\ \text{CTR: } ctr_i &= IV + i, t_i = \mathbb{E}_k(ctr_i), c_i = t_i \oplus m_i \end{aligned}$$

Cryptanalysis

$$\text{Pile-up lemma: } Pr(Z_1 \oplus \dots \oplus Z_n = 0) = \frac{1}{2} + 2^{n-1} \prod_{i=1}^n \varepsilon_i$$

Hash Functions

$$\begin{aligned} \text{First preimage: } Pr(m_i | d = h(m_i)) &\approx \frac{q}{|D|} \\ \text{Second preimage: } Pr(h(m_i) = h(m)) &= \frac{q-1}{|D|} \\ \text{Collision: } Pr(\text{no collisions}) &= e^{-\frac{q(q-1)}{2|D|}} \implies q \leq 1.774\sqrt{|D|} \end{aligned}$$

Algebraic Structures

Elliptic Curves

Public Key Cryptosystems

Montgomery Multiplication

Number Theoretical Cryptanalysis

Misc