

Cryptography and Architectures for Computer Security - Cheat Sheet

Information Theory

$$Pr(C = c) = \sum_{k:c \in \{\mathbb{E}_k(m), \forall m \in \mathcal{M}\}} Pr(K = k) Pr(P = \mathbb{D}_k(c))$$

$$\textbf{Perfect secrecy } Pr(P = m | C = c) = Pr(P = m) \implies |\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$$

$$\textbf{Entropy } H(X) = - \sum_{i=1}^n p_i \log_2 p_i \quad (p_i \log_2 p_i = 0 \text{ for } p_i = 0)$$

$$H(X, Y) = - \sum_{i=1}^n \sum_{j=1}^m Pr(X = x_i, Y = y_j) \log_2 Pr(X = x_i, Y = y_j)$$

$$H(X|Y = y) = - \sum_{i=1}^n \sum_{j=1}^m Pr(X = x_i | Y = y) \log_2 Pr(X = x_i | Y = y)$$

$$H(X|Y) = - \sum_{i=1}^n \sum_{j=1}^m Pr(Y = y_j) Pr(X = x_i, Y = y_j) \log_2 Pr(X = x_i | Y = y_j)$$

$$H(X) + H(Y) \geq H(X, Y); H(X, Y) = H(Y) + H(X|Y); H(X|Y) \leq H(X)$$

$$\textbf{Key equivocation } H(K|C) = H(P) + H(K) - H(C)$$

$$\textbf{Language redundancy } R_L = 1 - \frac{H_L}{\log_2 |\mathcal{M}|}$$

$$\textbf{Spurious keys } \bar{s}_n \geq \frac{|\mathcal{K}|}{|\mathcal{M}|^{nR_L}} - 1$$

$$\textbf{Unicity distance } n_0 \approx \frac{\log_2 |\mathcal{K}|}{R_L \log_2 |\mathcal{M}|}$$

Symmetric Ciphers

Modes of Operation

$$\textbf{ECB } c_i = \mathbb{E}_k(m_i)$$

$$\textbf{CBC } c_0 = IV, c_i = \mathbb{E}_k(m_i \oplus c_{i-1})$$

$$\textbf{CFB/OFB } ISR_0 = IV, OSR_i = \mathbb{E}_k(ISR_{i-1}), c_i = m_i \oplus \text{j-th leftmost bits of } OSR_i$$

$$\textbf{CTR } ctr_i = IV + i, t_i = \mathbb{E}_k(ctr_i), c_i = t_i \oplus m_i$$

Cryptanalysis

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

Hash Functions

$$\textbf{First preimage } Pr(m_i | d = h(m_i)) \approx \frac{q}{|D|}$$

$$\textbf{Second preimage } Pr(h(m_i) = h(m)) = \frac{q-1}{|D|}$$

$$\textbf{Collision } Pr(\text{no collisions}) = e^{-\frac{q(q-1)}{2|D|}} \implies q \leq 1.774\sqrt{|D|}$$

Algebraic Structures

$$\varphi(n) = |\{x \in \mathbb{N} : 1 \leq x \leq n-1, \gcd(n, x) = 1\}|$$

$$\varphi(nm) = \varphi(n)\varphi(m) \text{ for } \gcd(n, m) = 1, \varphi(p^k) = p^k - p^{k-1}$$

$$\forall x \in \mathbb{Z}_n^* \quad x^{\varphi(n)} \equiv_n 1, x^{-1} \equiv_n x^{\varphi(n)-1}$$

$$\textbf{CRT } X = (\sum M_i M'_i x_i) \bmod N, M_i = \frac{N}{n_i}, M'_i = M_i^{-1} \bmod n_i$$

$$\sum_{d:d|n} N_d(p) d = p^n = \deg(x^{p^n} - x)$$

$$M_d(p) = \frac{\varphi(p^n-1)}{d}$$

$$\textbf{Irreducibility } \gcd(f(x), x^{p^h} - x), h \leq \lfloor \frac{\deg(f(x))}{2} \rfloor$$

Elliptic Curves

$$\text{For } \mathbb{K} = \mathbb{F}_p, p \geq 3: \Delta = 4a^3 + 27b^2 \neq 0$$

$$\mathbb{E}(\mathbb{F}_p) : y^2 = x^3 + ax + b \text{ for } a, b \in \mathbb{F}_p, p \geq 3$$

$$x_3 = (\frac{y_1-y_2}{x_1-x_2})^2 - x_1 - x_2, y_3 = (\frac{y_1-y_2}{x_1-x_2})(x_1 - x_3) - y_1$$

$$x_4 = (\frac{3x_1^2+a}{2y_1})^2 - 2x_1, y_4 = -y_1 + (\frac{3x_1^2+a}{2y_1})(x_1 - x_4)$$

$$-P_1 = (x_1, -y_1)$$

$$\mathbb{E}(\mathbb{F}_{2^m}) : y^2 + xy = x^3 + ax^2 + b \text{ for } a, b \in \mathbb{F}_{2^m}, \Delta = b \neq 0$$

$$x_3 = (\frac{y_1+y_2}{x_1+x_2})^2 + (\frac{y_1+y_2}{x_1+x_2}) + x_1 + x_2 + a, y_3 = (\frac{y_1+y_2}{x_1+x_2})(x_1 + x_3) + x_3 + y_1$$

$$x_4 = x_1^2 + \frac{b}{x_1^2}, y_4 = x_1^2 + (x_1 + \frac{y_1}{x_1})x_3 + x_3$$

$$-P_1 = (x_1, x_1 + y_1)$$

Public Key Cryptosystems

RSA

$$\textbf{Keys } k_{pub} = \langle n, e \rangle, k_{priv} = \langle p, q, \varphi(n), d \rangle$$

$$n = p \cdot q, \gcd(e, \varphi(n)) = 1, d = e^{-1} \mod \varphi(n)$$

$$c = m^e \mod \varphi(n) \mod n, m = c^d \mod \varphi(n) \mod n$$

$$\textbf{CRT } m_p \equiv_p c^d \mod p^{-1}, m_q \equiv_q c^d \mod q^{-1}, m \equiv_n m_p q (q^{-1} \mod p) + m_q p (p^{-1} \mod p)$$

ElGamal

$$\textbf{Keys } k_{pub} = \langle n, g, g^s \rangle, k_{priv} = \langle s \rangle$$

$$ctx = \langle \gamma, \delta \rangle = \langle g^l, ptx(g^s)^l \rangle, ptx = \gamma^{n-s} \delta$$

$$sign = \langle ptx, \langle \gamma, \delta \rangle \rangle = \langle ptx, g^l, l^{-1}(h(m) - s \cdot h(\gamma)) \mod n \rangle$$

$$\text{signature is valid iff } (g^s)^{h(\gamma)} \cdot \gamma^\delta = g^{h(ctx)}$$

ECC-ElGamal

$$\textbf{Keys } k_{pub} = \langle n, P, [k_{priv}]P \rangle, k_{priv} \in \mathbb{Z}_n$$

$$ctx = \langle \gamma, \delta \rangle = \langle [r]P, M + [r]k_{pub,B} \rangle, [r]k_{pub,B} = [k_{priv,B}]\gamma = [k_{priv,B}]([r]P) \rightarrow ptx = \delta - [k_{priv,B}]\gamma$$

DSS-DSA

$$\textbf{Keys } k_{pub} = \langle p, q, g, g^s \rangle, k_{priv} = (s); q|(p-1), q = |\langle g \rangle|$$

Montgomery Multiplication

$$R' \equiv R^{-1} \mod N, N' \equiv -N^{-1} \mod R$$

$$\tilde{x} = \mu(x) = xR \mod N, n = \mu^{-1}(\tilde{x}) = \tilde{x}R' \mod N$$

$$t' = tN, t \equiv_b (-N_0)^{-1}x_0 \equiv_b N'_0x_0$$

Number Theoretical Cryptanalysis

Primality test

Fermat n is composite $\implies a^{n-1} \not\equiv_n 1$ with probability $> \frac{1}{2}$

Miller-Rabin $n-1 = d2^r : a^d \not\equiv_n \pm 1$ and $a^{d2^r} \not\equiv -1 \implies n$ is composite ($r \leq s-1$)

Factoring

Fermat $x = \lceil \sqrt{n} \rceil, y = x^2 - n$, until y is a perfect square $y = y + 2x + 1, x = x + 1$, then the factors are $x \pm \sqrt{y}$

Pollard's ρ pick a, b at random (e.g $x_0 = 2, x_i = x_{i-1}^2 + 1 \pmod n$), if $\gcd(a - b, n) \neq 1$ the result is a factor

Pollard's p-1 p B-power-smooth, $a = 2^{B!}$, so $p = \gcd(a - 1, n)$

DLog

BSGS $b = g^x \rightarrow \beta(g^{-\lceil \sqrt{n} \rceil})^i = g^j, x = i\lceil \sqrt{n} \rceil + j$

Polig-Hellman for each prime factor $\eta = g^{\frac{n}{p}}, \gamma_i = \gamma_{i-1} g^{l_{i-1} p^{i-1}}, \delta_i = (\beta \gamma_i^{-1})^{\frac{n}{p^{i+1}}}, l_i = \log_{\eta} \delta_i$

Misc

Convert to power of 2 $x = 2^n \Leftrightarrow n = \frac{\ln(x)}{\ln(2)}$