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

Modes of Operation

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

Cryptanalysis

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

Hash Functions

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

Algebraic Structures

Elliptic Curves

$\mathbb{E}(\mathbb{F}_p) : y^2 = x^3 + ax + b$ for $a, b \in \mathbb{F}_p, p \geq 3$
$x_3 = (\frac{y_1-y_2}{x_1-x_2})^2 - x_1 - x_2$, $y_3 = (\frac{y_1-y_2}{x_1-x_2})(x_1 - x_3) - y_1$
$x_4 = (\frac{3x_1^2+a}{2y_1})^2 - 2x_1$, $y_4 = -y_1 + (\frac{3x_1^2+a}{2y_1})(x_1 - x_4)$
$-P_1 = (x_{1,-y_1})$

$\mathbb{E}(\mathbb{F}_{2^m}) : y^2 + xy = x^3 + ax^2 + b$ for $a, b \in \mathbb{F}_{2^m}, b \neq 0$
$x_3 = (\frac{y_1+y_2}{x_1+x_2})^2 + (\frac{y_1+y_2}{x_1+x_2}) + x_1 + x_2 + a$, $y_3 = (\frac{y_1+y_2}{x_1+x_2})(x_1 + x_3) + x_3 + y_1$
$x_4 = x_1^2 + \frac{b}{x_1^2}$, $y_4 = x_1^2 + (x_1 + \frac{y_1}{x_1})x_3 + x_3$
$-P_1 = (x_1, x_1 + y_1)$

Public Key Cryptosystems

RSA

Keys $k_{pub} = (n, e)$, $k_{priv} = (p, q, \varphi(n), d)$
$n = p \cdot q$, $gcd(e, \varphi(n)) = 1$, $d = e^{-1} \mod \varphi(n)$
$c = m^{e \mod \varphi(n)} \mod n$, $m = c^{d \mod \varphi(n)} \mod n$
CRT $m_p \equiv_p c^{d \mod p-1}$, $m_q \equiv_q c^{d \mod q-1}$, $m \equiv_n m_p q(q^{-1} \mod p) + m_q p(p^{-1} \mod p)$

Montgomery Multiplication

Number Theoretical Cryptanalysis

Primality test

Fermat n is composite $\implies a^{n-1} \not\equiv_n 1$ with probability $> \frac{1}{2}$
Miller-Rabin $n - 1 = d2^s : a^d \not\equiv_n \pm 1$ and $a^{d2^r} \not\equiv -1 \implies n$ is composite

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 $\boldsymbol{\rho}$ pick a, b at random (e.g $x_0 = 2, x_i = x_{i-1}^2 + 1 \mod n$)), 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

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