1 Secure Ciphers

A cipher is perfectly safe if $P(M = m \mid C = c) = P(M = m)$, where M and C refer to random variables for message and ciphertext, and m and c are particular messages and ciphertexts.
This can be interpreted as not gaining any information about what the message might be by intercepting a ciphertext.

This definition is equivalent to:
$\forall m,\ n \in \mathcal{M},\ \forall c \in \mathcal{C},\ P(Enc_k(m) = c) = P(Enc_k(n) = c)$, where $\mathcal{M}$ is the space of all possible messages, and $\mathcal{C}$ is the space of all possible ciphertexts.

It is also equivalent to this game:
Let $\mathcal{A}$ be an adversary and $\mathcal{C}$, the defender.
The game works as follows:

1. $\mathcal{A}$ chooses m_0 and m_1 and sends them to $\mathcal{C}$.
2. $\mathcal{C}$ then randomly chooses $b_{\mathcal{C}} \in \{0, 1\}$ and sends back $Enc_k(m_{b_{\mathcal{C}}}) = c$.
3. $\mathcal{A}$ finally chooses $b_{\mathcal{A}} \in \{0, 1\}$ and wins the game if $b_{\mathcal{A}} = b_{\mathcal{C}}$.

The cipher is valid if $\forall \mathcal{A},\ P(\mathcal{A}\ wins) = \frac{1}{2}$.

2 RSA

2.1 Preparation

1. Choose two random primes p and q
2. Let $n = p \cdot q$
3. Choose e such that $1 < e < \phi(n)$ and $gcd(e, \phi(n)) = 1$, where $\phi(n)$ is Euler's totient function.
4. Determine $d \equiv (e^{-1})\ (mod\ \phi(n))$, the modular inverse of e modulo $\phi(n)$ i.e. the unique d such that $d \cdot e \equiv 1\ (mod\ \phi(n))$
   Since e was chosen such that $gcd(e, \phi(n)) = 1$, d can be determined using Euclid's Extended Algorithm.

2.1.1 Public Key

The public information consists of n and e.

2.1.2 Private Key

The private information constists of d.

2.2 Encryption

Assume Bob wants to send information to Alice, and Alice has published her public key: n and e.
Let m be the message Bob wants to transmit, with $0 \leq m < n$.
Bob first computes $c \equiv m^e \ (mod\ n)$ and then sends c to Alice.

2.3 Decryption

After Alice has received c from Bob, she can decode the original message m as $m \equiv c^d \ (mod\ n)$.

2.3.1 Proof

Decrypting the message, we have $c^d \equiv (m^e)^d \equiv m^{e \cdot d} \ (mod\ n)$
Remember that d was chosen such that $e \cdot d \equiv 1 \ (mod\ \phi(n))$.
Therefore, we can write $e \cdot d$ as $k * \phi(n) + 1$, where $k \in \mathbb{N}$. Substituting, we have $m^{e \cdot d} = m^{k*\phi(n)+1} = m^{k*\phi(n)} \cdot m^1$.
Euler's theorem states that and $a^{\phi(n)} \equiv 1 \ (mod\ n) \ \forall a$ such that $gcd(a, n) = 1$.
As such, $m^{k \cdot \phi(n)} = (m^{\phi(n)})^k \equiv (1)^k \equiv 1 \ (mod\ n)$.
Then $m^{k*\phi(n)} \cdot m^1 \equiv m \ (mod\ n) \implies c^d \equiv m \ (mod\ n)$

3 Random Number Generators

A random number generator is a function $G : \{0,\ 1\}^s \to \{0,\ 1\}^l$ where $l << s$.

3.1 Secure RNG

Consider the following game, where $\mathcal{C}$ is the defender:

1. $\mathcal{C}$ randomly chooses $b \in \{0,\ 1\}$
   (a) if $b = 0$, then $\mathcal{C}$ randomly chooses $r \in \{0,\ 1\}^l$ and sends $o = r$ to $\mathcal{A}$.
   (b) if $b = 1$, then $\mathcal{C}$ randomly chooses $r \in \{0,\ 1\}^s$ and sends $o = G(r)$ to $\mathcal{A}$.
2. $\mathcal{A}$ receives o and tries to guess b as b'. $\mathcal{A}$ wins the game if $b' = b$.

G is a secure random number generator if $\forall \mathcal{A}$ adversary, $\mathcal{A}$ has a negligible advantage in this game.

$\mathcal{A}$ has a negligible advantage in this game $\iff P(\mathcal{A}\ wins) \leq \frac{1}{2} + u$, where u is negligible.
The function u is negligible if it is an inverse of an exponential function defined on the parameters of the generator.
For instance, $u = \frac{1}{2^s}$ is negligible, while $u = \frac{1}{s^2}$ and $u = \frac{1}{3}$ are not negligible.