A Public-Key Encryption Scheme is a triple, (G, E, D), of probabilistic polynomial-time algorithms satisfying the following conditions:

① Key Generation Algorithm: a probabilistic expected polynomial-time algorithm G, which, on input 1^k (the security parameter) produces a pair (e, d) where e is called the public key, and d is the corresponding private key. $((e,d) \in G(1^k))$.

② An Encryption Algorithm: a probabilistic polynomial-time algorithm E which takes as input a security parameter 1^k, a public-key e from the range of $G(1^k)$ and string $m \in \{0,1\}^k$ called the plaintext, and produces as output string $c \in \{0,1\}^*$ called the ciphertext. $(c \in E(1^k, e, m))$

③ A Decryption Algorithm: a probabilistic polynomial time algorithm D that takes as inputs a security parameter 1^k, a private-key d from the range of $G(1^k)$, and a ciphertext c from the range of $E(1^k, e, m)$, and produces as output a string $m' \in \{0,1\}^*$, such that for every pair (e,d) in the range of $G(1^k)$, for every m, for every $c \in D(1^k, e, m)$, the $P_r[D(1^k, d, c) \neq m]$ is negligible.

④ (G, E, D) is semantically secure.

Messages of length not equal to k (the length of the encryption key) are encrypted by breaking them into blocks of length k and possibly padding the last block:

$E_e(\alpha_1 \cdots \alpha_l \alpha_{l+1}) = E_e(\alpha_1) \cdots E_e(\alpha_l) \cdot E_e(\alpha_{l+1} p)$

where $|\alpha_1| = \cdots = |\alpha_l| = k$, $|\alpha_{l+1}| \leq k$, and p is some standard padding of length $k - |\alpha_{l+1}|$.

Polynomial Time Indistinguishability: We say that a public key cryptosystem (G, E, D) is polynomial time indistinguishable if for every PPT M, A, and for every polynomial Q, $\forall$ sufficiently large k

$$\Pr[A(1^k, e, m_0, m_1, c) = m \mid (e,d) \xleftarrow{\$} G(1^k); \{m_0, m_1\} \xleftarrow{\$} M(1^k); m \xleftarrow{\$} \{m_0, m_1\}; c \xleftarrow{\$} E(e,m)] < \frac{1}{2} + \frac{1}{Q(k)}$$

In other words, it is impossible in polynomial in k time to find two messages m_0, m_1 such that a polynomial time algorithm can distinguish between $c \in E(e, m_0)$ and $c \in E(e, m_1)$.

Any encryption scheme in which the encryption algorithm E is deterministic immediately fails to pass this security requirement. Given f, m_0, m_1, and $c \in \{f(m_0), f(m_1)\}$ it is trivial to decide whether $c = f(m_0)$ or $c = f(m_1)$.

Semantic Security: Consider the following two games. Let $h: M \to \{0,1\}^*$, where M is a message space in which we can sample in polynomial time.

Game 1: Adversary is given the information that some $m \in M(1^k)$ will be encrypted. Adversary has to guess $h(m)$.

Game 2: Adversary is given $\alpha \in E(m)$, for some $m \in M(1^k)$. Adversary has to guess $h(m)$.

The adversary should not gain any advantage or information from having seen the ciphertext resulting from the encryption algorithm.

We say that an encryption scheme (G, E, D) is <u>semantically secure</u> if for all PPT algorithms M and A, functions h, polynomials Q there is a PPT B such that for sufficiently large k,

$$\Pr\left[A(1^k, c, e) = h(m) \;\middle|\; (e,d) \xleftarrow{\$} G(1^k);\ m \xleftarrow{\$} M(1^k);\ c \xleftarrow{\$} E(e,m)\right] \leq \Pr\left[B(1^k) = h(m) \;\middle|\; m \xleftarrow{\$} M(1^k)\right] + \frac{1}{Q(k)}$$

Here, Game 1 is represented by PTM B, and Game 2 by PTM A. Again, this can only hold true when the encryption algorithm is a probabilistic one which selects one of many possible encodings for a message; otherwise, if E were deterministic, and $M = \{0,1\}$, then any adversary would have 100% chance of guessing correctly $h(m)$ for $m \in M$ by simply testing whether $E(0) = c$ or $E(1) = c$.

A Public Key Cryptosystem posses Indistinguishable Security if and only if it posses Semantic Security.

If p denotes an odd prime, then the Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 1 if a is a quadratic residue, -1 if a is a quadratic nonresidue modulo p, and 0 if $p \mid a$.

Let p be an odd prime, then

① $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$

② $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

③ $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

④ If $(a,p)=1$ then $\left(\frac{a^2}{p}\right)=1$, $\left(\frac{a^2b}{p}\right)=\left(\frac{b}{p}\right)$

⑤ $\left(\frac{1}{p}\right)=1$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

Proof of ①: Assuming that $\left(\frac{a}{p}\right)=1 \Rightarrow x^2 \equiv a \pmod{p}$ has a solution. Let x_0 be the solution. By Fermat's Little theorem: $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}$.

Assuming that $\left(\frac{a}{p}\right) = -1 \Rightarrow x^2 \equiv a \pmod{p}$ has no solution. We proceed as in the proof of Wilson's theorem. To each j satisfying $1 \le j < p$, choose j', $1 \le j' < p$, so that $jj' \equiv a \pmod{p}$. We pair j with j'. We note that $j \not\equiv j' \pmod{p}$, since the congruence $x^2 \equiv a \pmod{p}$ has no solution. The combined contribution of j and j' to $(p-1)!$ is $jj' \equiv a \pmod{p}$. Since there are $(p-1)/2$ pairs j, j', it follows that $a^{(p-1)/2} \equiv (p-1)! \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod{p}$ using Wilson's theorem.

②–⑤ can be obtained from the formula in ①

The Jacobi Symbol: Let Q be positive and odd, so that $Q = q_1 q_2 \cdots q_s$ where the q_j are odd primes, not necessarily distinct. Then the Jacobi symbol $\left(\frac{P}{Q}\right)$ is defined by $\left(\frac{P}{Q}\right) = \prod_{j=1}^{s} \left(\frac{P}{q_j}\right)$ where $\left(\frac{P}{q_j}\right)$ is the Legendre symbol.

If Q is an odd prime, the Jacobi symbol and Legendre symbol are indistinguishable. If $(P,Q) > 1$, then $\left(\frac{P}{Q}\right) = 0$, whereas if $(P,Q) = 1$, then $\left(\frac{P}{Q}\right) = \pm 1$. Moreover, if P is a quadratic residue modulo an odd number Q, then P is a quadratic residue modulo each prime q_j dividing Q, so that $\left(\frac{P}{q_j}\right) = 1$ for each j, and hence $\left(\frac{P}{Q}\right) = 1$. However, $\left(\frac{P}{Q}\right) = 1$ does not imply that P is a quadratic residue of Q. For example, $\left(\frac{2}{15}\right) = 1$, but $x^2 \equiv 2 \pmod{15}$ has no solution. If Q is odd then a is a quadratic residue $(\bmod Q)$ if and only if $\left(\frac{a}{p}\right) = 1$ for every p dividing Q. Let $p_1, p_2, \ldots, p_r$ denote the distinct primes dividing an odd number Q. Then the reduced residue classes modulo Q are partitioned into 2^r subsets of $\phi(Q)/2^r$ classes each, according to the values of $\left(\frac{a}{p_1}\right), \left(\frac{a}{p_2}\right), \ldots, \left(\frac{a}{p_r}\right)$. Of these subsets, the particular one for which $\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right) = \cdots = \left(\frac{a}{p_r}\right) = 1$ is the set of quadratic residues $(\bmod Q)$.

Suppose that Q and Q' are odd and positive. Then

① $\left(\frac{P}{Q}\right)\left(\frac{P}{Q'}\right) = \left(\frac{P}{QQ'}\right)$,

② $\left(\frac{P}{Q}\right)\left(\frac{P'}{Q}\right) = \left(\frac{PP'}{Q}\right)$,

③ if $(P,Q)=1$, then $\left(\frac{P^2}{Q}\right) = \left(\frac{P}{Q^2}\right) = 1$,

④ if $(PP', QQ') = 1$, then $\left(\frac{P'P^2}{Q'Q^2}\right) = \left(\frac{P'}{Q'}\right)$.

⑤ $P' \equiv P \pmod{Q}$ implies $\left(\frac{P'}{Q}\right) = \left(\frac{P}{Q}\right)$.

If Q is odd and $Q > 0$, then

$$\left(\frac{-1}{Q}\right) = (-1)^{(Q-1)/2} \quad \text{and} \quad \left(\frac{2}{Q}\right) = (-1)^{(Q^2-1)/8}.$$

If P and Q are odd and positive and if $(P,Q) = 1$, then $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\left(\frac{P-1}{2}\cdot\frac{Q-1}{2}\right)}$.

We can apply the above formulas for computing the Jacobi symbol in polynomial time. For example:

$$\left(\frac{105}{317}\right) = \left(\frac{317}{105}\right) = \left(\frac{2}{105}\right) = 1.$$