Allgemein:
Das RSA-Verschlüsselungsverfahren ist ein häufig benutztes Verschlüsselungsverfahren, weil es sehr sicher ist. Es gehört zu der Klasse der asymmetrischen Verschlüsselungsverfahren.
Die Verschlüsselung besteht aus zwei Schlüsseln, einem *öffentlichen* und einem *privaten* Schlüssel.
Mit dem öffentlichen Schlüssel kann man Nachrichten verschlüsseln, aber nicht entschlüsseln. Deshalb wird dieser Schlüssel öffentlich (daher sein Name) zur Verfügung gestellt, z. B. im Internet. Hier kann den Schlüssel dann jeder benutzen, um Nachrichten zu verschlüsseln, die aber nur der Empfänger (= derjenige, der den öffentlichen Schlüssel anbietet) wieder entschlüsseln kann.
Zum Entschlüsseln braucht man den privaten Schlüssel, und den kennt nur der Empfänger.
Man kann sich das auch so vorstellen: n ist eine Straße mit Hausnummer, e ist die Postleitzahl – dies ist der öffentliche Schlüssel, den jeder kennen darf. Damit kann jeder der Person einen Brief schreiben.
Aber nur der Empfänger kann den Brief lesen, weil sonst niemand den Schlüssel d (privater Schlüssel) für den Briefkasten des Empfängers hat.

Nun sehen wir an einem Beispiel, wie die Verschlüsselung abläuft. Die Regierung der Bundesrepublik Deutschland möchte von der amerikanischen Regierung wichtige militärische Daten erhalten. Diese Daten sollen die Amerikaner verschlüsselt schicken. Dazu brauchen die Amerikaner aber die Adresse, also Straße (n) und Postleitzahl (e). Diese Adresse (= öffentlicher Schlüssel) darf auch jeder wissen, denn es darf jeder der deutschen Regierung Briefe schreiben.

1. Schritt: Öffentlichen Schlüssel anlegen

a) n ermitteln:
n ist eine Zahl, die ein Produkt von zwei Primzahlen ist (z. B. 3 und 7), also gilt:
n = q * p = 3 * 7 = 21

b) e ermitteln:
e ist eine beliebige Zahl, die aber mit (p-1)(q-1), also (3-1)(7-1)=12 keinen gemeinsamen Teiler außer 1 haben darf. Das ist z. B. 5.

Damit haben wir schon den öffentlichen Schlüssel:
n = 21 und e = 5. Den schicken wir den Amerikanern.

2. Schritt: Privaten Schlüssel anlegen:

Der private Schlüssel ist die Zahl d, sie ist eine Zahl $\leq$ (p-1)(q-1), für die gilt:

$$ed \bmod (p-1)(q-1) = 1$$

Man kann d berechnen durch:

$$e*d = s(p-1)(q-1)+1,$$

wobei sich s automatisch ergibt.
=> 5d = 12s+1 <=> d = 5 und s = 2
Und in der Tat gilt: 5*5 mod (3-1)(7-1) = 1
Diesen Schlüssel kann man nur anlegen, wenn man p und q kennt, diese gehören aber nicht zum öffentlichen Schlüssel. Weil der private Schlüssel zum Entschlüsseln wichtig ist, kann keiner nur mit dem öffentlichen Schlüssel die Nachricht entschlüsseln.

3. Schritt: Nachricht verschlüsseln

a) Nachricht in Zahlen umwandeln:

Es können nur Zahlen verschlüsselt werden, also wird die Nachricht mit der Tabelle in Zahlen umgewandelt:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Die Nachricht lautet:
„IRAK“, als Zahl geschrieben: „09 18 01 11“

b) Nachricht verschlüsseln:
Die Zahl kann nun mit der Formel

$$verschlüsselung = nachricht^{e} \bmod n$$

verschlüsselt werden. Allerdings ist die Zahl größer als n. Deshalb muss die Zahl zerlegt werden. Zunächst wird „09“ verschlüsselt:

$$verschlüsselung = 09^{5} \bmod 21 = 18$$

Verschlüssele jetzt selbst den Rest der Zahl, immer zwei Ziffern gleichzeitig:

Zahl zu verschlüsseln	Formel	Ergebnis/Verschlüsselung
09	$09^{5} \bmod 21$	18
18	$18^{5} \bmod 21$	
01		
11		

4. Schritt: Nachricht entschlüsseln:

a) Nachricht entschlüsseln:
Die Amerikaner haben uns nun die Nachricht geschickt, die lautet
18 __ __ __ (trage hier deine Ergebnisse ein)
Die Zahlen müssen wir jetzt einzeln entschlüsseln. Wir beginnen mit der 18. Dazu nehmen wir die Formel

$$entschlüsselung = geheimnachricht^{d} \bmod n$$

Die Formel können nur wir lösen, weil sonst niemand die Zahl d kennt, und zwar so:

$$entschlüsselung = 18^{5} \bmod 21 = 09$$

Die Zahl 09 stimmt mit der ursprünglichen Nachricht überein. Die Entschlüsselung war also korrekt.
Entschlüssele nun selbst die übrigen Zahlen:

Zahl zu entschlüsseln	Formel	Ergebnis/Entschlüsselung
18	$18^{5} \bmod 21$	09

b) Nachricht in Buchstaben umwandeln:
Nach der Tabelle kann nun die Nachricht: 09 __ __ __
in Buchstaben umgewandelt werden: I __ __ __,

das Ergebnis ist (bei richtiger Rechnung): „IRAK“.

Wir haben nun die Nachricht verschlüsselt und wieder entschlüsselt. Die verschlüsselte Nachricht konnte keiner verstehen und auch nicht entschlüsseln, weil er nicht den privaten Schlüssel (d) kannte.
Jetzt habe ich nur gesagt, mit welcher Formel man die Verschlüsselung macht, aber noch nicht dass und warum/wie die Formel funktioniert (also warum man nach der Entschlüsselung tatsächlich wieder die Original-Nachricht erhält) und auch nicht, warum denn der verschlüsselte Text so sicher und (fast) nicht knackbar ist. Dies zeige ich im Folgenden:

Verifikation der korrekten Ver- und Entschlüsselung:
Vor 300 Jahren kam ein Mathematiker (Euler) auf die Welt, der einen seltsamen Satz entwickelte. Der sagte, unter bestimmten Bedingungen gilt:

$$m^{s(p-1)(q-1)+1} \bmod n = m$$

Warum das so ist, wie er darauf kam? Das müssen wir Durchschnittsmenschen mit einem IQ $\neq 250$ mit einem Schulterzucken hinnehmen.
Daraus ergibt sich dann

$$entschlüsselung = nachricht^{d} \bmod n = (nachricht^{e})^{d} \bmod n = nachricht^{ed} \bmod n$$

und nach der Wahl von e und d (s. oben) ergibt sich mit Euler:

$$nachricht^{ed} \bmod n = nachricht$$

Nach den oben angewandten Formeln ergibt sich also tatsächlich zunächst eine Verschlüsselung und dann eine Entschlüsselung, wobei die Entschlüsselung mit der ursprünglichen Nachricht übereinstimmt.

Sicherheit und Sicherheitslücken:
Die Verschlüsselung ist so sicher, weil man zum Entschlüsseln auf jeden Fall den geheimen Schlüssel d kennen muss. Kennt man den nicht, ist eine Verschlüsselung unmöglich.
Der private Schlüssel wird aus

$$e*d = s(p-1)(q-1)+1$$

berechnet (s. oben). Allerdings ist e bekannt und d sowie s ergeben sich erst beim Rechnen. Das einzige, was man zum Errechnen von d braucht, sind also p und q. Die kennen wir nicht. Aber wir kennen n, und es gilt n = pq, wobei p und q Primzahlen sind.
Man kann also d errechnen (und damit die Verschlüsselung knacken!), indem man q und p findet – die Primzahlen, deren Produkt n ergibt. Man *faktorisiert* n.

Stell dir nun vor, du bist ein Russe und weil du heute noch nicht so viel Vodka getrunken hast, bist du sogar einigermaßen klar bei Verstand. Da empfängst du zufällig eine Nachricht, die die Amerikaner den Deutschen schicken, aber die Nachricht ist verschlüsselt:

01 18 12

Du weißt aber – weil du den Deutschen auch Nachrichten geschickt hast –, dass der öffentliche Schlüssel der Deutschen so aussieht:
n = 35 und e = 11.
Versuche nun, die Verschlüsselung zu knacken:

1. Faktorisiere n=35 (d. h., finde die Primzahlen, deren Produkt n ergibt). Es ergibt sich

   p = __

   q = __

2. Errechne den geheimen Schlüssel d:

e*d = s(__-1)(__-1)+1 =>

d = __

3. Entschlüssel nun die Nachricht, (immer zwei Zahlen zusammen):

Zahl zu entschlüsseln	Formel	Ergebnis/Entschlüsselung
01		
18		
12		

Es ergibt sich als Buchstaben: __ __ __
Verschlüssel diese Buchstaben zur Kontrolle mit dem öffentlichen Schlüssel der Deutschen um herauszufinden, ob du richtig gearbeitet hast. Erhältst du als Verschlüsselung wieder 01 18 12, hast du richtig entschlüsselt.

Du siehst, dass die RSA-Verschlüsselung nicht unknackbar ist. Jeder, der n faktorisieren kann, kann auch die Nachricht entschlüsseln. Deshalb werden in der Praxis sehr große Primzahlen gewählt, deren Produkt man nicht mehr so leicht faktorisieren kann. Wenn das Produkt z. B.

n = 415 758 465 533 848 642 967

ist, ist die Faktorisierung schon sehr zeitaufwändig. Aber theoretisch möglich!
In der Praxis ist es aber nahezu unmöglich, eine sehr große Zahl zu faktorisieren.
Es gibt auch noch andere Möglichkeiten, RSA zu entschlüsseln, aber diese sind ebenso schwierig lösbar.
Es ist auch möglich, dass es eine ganz einfache Dechiffrierung ohne privaten Schlüssel gibt, die bis jetzt noch niemand entdeckt hat. Wir können da nicht sicher sein.

Bis jetzt ist das RSA-Verfahren ein sehr sicheres und doch leicht handhabbares Verfahren in der Verschlüsselungstechnik.