RSA public key encryption

(Rivest, Shamir, Adleman 1977)

It relies on Euler's Theorem: If a and n are coprime, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

RSA setup: Pick two distinct primes p and q (about 1000 digits each to be safe). Also choose (randomly) an invertible element e in $\mathbb{Z}$ mod $\varphi(pq)$ (here $\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$) and then you find e^{-1} mod $\varphi(pq)$, call it d, i.e. $de \equiv 1 \bmod \varphi(pq)$.

Calculate $n = pq$.

Public key: (n, e) publish

Private key: (n, d) keep secret!

Messages over an alphabet, say 26 letter alphabet, are broken into m-letter units, each of which is encrypted into an ℓ-letter ciphertext unit

Example: $m = 3$, $\ell = 4$

plaintext: FUN $\longleftrightarrow$ $\underset{F}{5}\cdot 26^2 + \underset{U}{20}\cdot 26 + \underset{N}{13} = 3913$

Encryption: $x \longmapsto x^e \pmod{n}$

translated into a 4-letter unit

Decryption: take 4-letter unit and get its number, which will be $x^e \pmod n$

Calculate $(x^e)^d = x^{ed} \equiv x \pmod n$

Example: Take $p = 103$, $q = 97$, $n = 9991$

$\varphi(n) = 102 \cdot 96 = 9792$

Pick $e = 55$. Now find $d = e^{-1} \pmod{9792}$

$d = 4807$. Public: $(9991, 55)$

Private: $(9991, 4807)$

Now encrypt FUN $\leftrightarrow$ 3913

$\downarrow$

AIRH $\leftrightarrow$ $3913^{55} \pmod{9991} = 5870$

$= 0 \cdot 26^3 + 8 \cdot 26^2 + 17 \cdot 26 + 20$