Шифрование в системе RSA производится путём возведения исходного текста *X* () в степень открытого ключа *KО* по модулю большого числа *r*:

*Y* = *EKO*(*X*) = *X* *KO* mod *r*.

**Расшифрование производится путём возведения шифротекста *Y* в степень закрытого ключа *KС* по модулю *r* :**

*Y* *KC* mod *r* = (*X* *KO* mod *r*) *KC* mod *r* = *X* *KO·KC* mod *r* = *X* mod *r*.

Возможность получения исходного текста из зашифрованного обеспечивается свойством открытого и закрытого ключей, для которых должно выполняться равенство

(*KO·KC*)mod *φ*(*r*) = 1,

где *φ*(*r*) – функция Эйлера от *r*. Закрытый ключ является мультипликативным инверсным по модулю *φ*(*r*) для открытого. По теореме Эйлера

*a φ*(*r*) = 1 mod *r*,

где (*a*, *r*) = 1.

Известно, что если

*a* = *b* mod *r*,

то

*an*= *bn* mod *r.*

Из этого следует, что

*X n·φ*(*r*)= 1 mod *r.* (2)

Поскольку для модулярной арифметики справедливо

*m·a* = *m·b* mod *r* ***,***

то мы можем умножить левую и правую части равенства (2) на *X*:

*X n·φ*(*r*)+1= *X* mod *r.*

Если представить показатель степени *n·φ*(*r*)+1 как произведение значений *KO* и *KC*, то получим:

*KO·KC* = 1 mod *φ*(*r*).