Пусть m - некоторый текст (необязательно соответствующий PKCS паддингу), $c = E(m)$ - зашифрованный текст, длина текста - k байт. Обозначим за $B = 2^{8(k-1)}$. Пусть у нас есть оракул, отвечающий на следующий вопрос: соответствует ли текст m паддингу PKCS (оракул получает текст в зашифрованном виде, т.е. получает $E(m)$).
Перед тем, как описать алгоритм поиска m, сделаем нексолько замечаний: Пусть m_1 соответствует PKCS паддингу и пусть $s > 1$ - такое число, что $m_2 = m_1 s \bmod n$ - соответствует PKCS паддингу. Тогда:

- $m_1 \in \{[2B, 3B-1]\}$
- $m_2 \in \{[2B, 3B-1]\}$
- $m_2 = m_1 s - rn$, где r - некоторое натуральное число
- $\frac{2B-rn}{s} \leq m_2 \leq \frac{3B-1-rn}{s}$
- $r = \frac{m_1 s - m_2}{n}$
- $\frac{2Bs-3B+1}{n} \leq r \leq \frac{(3B-1)s-2B}{n}$

Пусть $s = \frac{n}{3B}$, тогда $r < 1$. Поэтому $s \geq \frac{n}{3B}$.
Опишем алгоритм, который по c находит m.

1. Начальный шаг.
   Найдём такое s_0, что $ms_0 \bmod n$ соответствует PKCS паддингу. Если m изначально соответствовало PKCS паддингу, то берем $s = 1$, иначе побираем s простым "угадыванием". Получаем следующее:
   - $c_0 \leftarrow c(s_0)^e \bmod n$
   - $M_0 \leftarrow \{[2B, 3B-1]\}$ - интервал, в который может входить ms_0
   - $i \leftarrow 1$ - номер иттерации алгоритма.
2. Поиск сообщения, соответствующего PKCS паддингу.
   2.1. Если $i = 1$, то:
   находим такое наименьшее $s_1 \geq \frac{n}{3B}$, что $c_0(s_i)^e \bmod n$ соответствует PKCS паддингу (почему $s_1 \geq \frac{n}{3B}$, мы объяснили выше).
   2.2. Если $i > 1$ и количество интервалов в M_{i-1} как минимум 2, то:
   находим такое наименьшее $s_i > s_{i-1}$, что $c_0(s_i)^e \bmod n$ соответствует PKCS паддингу.

2.3. Если $i > 1$ и количество интервалов в M_{i-1} равно 1 (т.е. $M_{i-1} = [a, b]$), то:
находим такие "небольшие"$r_i \geq 2\frac{bs_{i-1}-2B}{n}$ и $\frac{2B+r_in}{b} \leq s_i < \frac{3B+r_in}{a}$, что $c_0(s_i)^e \bmod n$ соответствует PKCS паддингу.

3. Сужение множества решений.
После того, как s_i было найдено, множество M_i ищется следующим образом:
$M_i \leftarrow \bigcup_{(a,b,r)}\{[max(a, \lceil\frac{2B+rn}{s_i}\rceil), min(b, \lfloor\frac{3B-1+rn}{s_i}\rfloor)]\}$ для всех $[a, b] \in M_{i-1}$ и $\frac{as_i-3B+1}{n} \leq r \leq \frac{bs_i-2B}{n}$.

4. Вычисление ответа.
Если M_i содержит один интервал длины 1 (т.е. $M_i = [a, a]$), то: $m \leftarrow a(s_0)^{-1} \bmod n$ и возвращаем m как решение (m можно найти с помощью расширенного алгоритма Евклида). Иначе, увеличить i на 1 и вернутся на шаг 2.

Корректность алгоритма доказывается по индукции. Более подробное доказательство, а так же оценку времени работы можно найти в оригинальной статье.