HTTPS Defense (RFC 5246)

Attacks discovered by Bleichenbacher and Klima et al. … can be avoided by treating incorrectly formatted message blocks … in a manner indistinguishable from correctly formatted RSA blocks.

In other words:

1. *Generate a string **R** of 46 random bytes*

2. *Decrypt the message to recover the plaintext M*

3. *If the PKCS#1 padding is not correct*

   *pre_master_secret = **R***