**Cryptographic Attacks**

Apart from the padding oracle and compression-based attacks on TLS, some attacks target the cryptographic algorithms directly. For the sake of completion, we discuss three such attacks here.

**LUCKY13 Attack**

The [Lucky13 attack](https://www.ieee-security.org/TC/SP2013/papers/4977a526.pdf) was reported in 2013 and exploits a timing difference in the MAC stage when the CBC mode is used. It is similar to padding oracle attacks. To prevent padding oracle attacks, TLS servers do not leak a verbose error message when the padding is incorrect. Additionally, the server computes a MAC even if the padding was incorrect to avoid detectable timing differences that would also enable padding oracle attacks. The Lucky13 attack exploits the fact that this MAC computation also includes the incorrect padding bytes, making the MAC computation take slightly longer in some cases. This subtle timing difference can be enough to leak whether the padding was valid or not, potentially leading to a full plaintext recovery. This attack was patched in 2013 by most libraries, making up-to-date libraries a sufficient countermeasure. Today, Lucky13 attacks do not play a role in real-life engagements.

**SWEET32 Attack**

[Sweet32](https://sweet32.info/) is a birthday attack against the block ciphers in TLS. The goal of birthday attacks is to find a collision in block ciphers with short block lengths of 64 bit. Older TLS versions utilize such block ciphers, for instance Triple-DES. To successfully find a collision, an attacker needs to capture multiple hundred gigabytes of traffic, making the attack last multiple days. The TLS connection would have to be kept alive for the duration of the attack. The attack was reported in 2016 and, just like with Lucky13, most libraries patched the underlying issues. The best countermeasure is using TLS 1.3, as TLS 1.3 eliminated all weak block ciphers with short block lengths.

**FREAK Attack**

The [Factoring RSA Export Keys (FREAK)](https://freakattack.com/) attack exploits weak encryption that was supported in older TLS versions. SSL 3.0 and TLS 1.0 included export cipher suites. These cipher suites are deliberately weak to comply with regulations in the United States that restricted the export of strong cryptographic software. Since these algorithms were already considered weak back in the 1990s, they can easily be broken today due to short key lengths. Servers vulnerable to the FREAK attack still support such RSA\_EXPORT cipher suites that are weak by today's standard and can be broken. Since export cipher suites were removed in TLS 1.2, a sufficient countermeasure is disabling support of TLS 1.1 and older.