Breaking CSS

CSS used for encryption of DVDs (introduced 1996, broken 1999)

combines 2 LFSRs (nonlinearly!)

key size: 40 bits (max allowed for US export)

LFSR-1	17 bits	(seed uses 16 bits of key)
LFSR-2	25 bits	(seed uses 24 bits of key)

CSS-PRG: add outputs from LFSRs **with carry** (nonlinear)

brute-force attack in time 2^{40} (hard but doable)

correlation attack in time 2^{16} (super easy!)

MPEG ⇝ Eve knows first x bytes of m (6-20 bytes)

⇝ can compute x bytes of PRG keystream

for each of the 2^{16} possible seeds for LFSR-1:

- generate x bytes using LFSR-1
- subtract from PRG
  ⇝ this would be output of LFSR-2
  possible output?
  NO: continue with next seed
  YES: likely found correct seed