GSM (Global System for Mobile communication)

GSM encryption ciphers

A5/0: No encryption

A5/1: Based on LFFRs (Linear Forward Shift Register), developed first, stronger and used in Europe and US, broken with known-plaintext attack

A5/2: Weakened A5/1, broken with real-time ciphertext-only attack

A5/3: KASUMI, new for 3G. A block cipher vulnerable to impossible differential attack and man-in-the-middle protocol attacks.

Deliberately weak cipher designs due to cost and politics.

Using the right primitives

Using the wrong crypto or homebrew crypto is bad (e.g. RC4 in WEP and TLS)

Sometimes people use the right ones wrong (e.g. seeing the penguin, AES-ECB)

Right crypto stop being right (e.g. MD5 and SHA1 broken)

Quantum computer poses a huge threat

Man-in-the-middle