Advanced Analogue and Digital Encryption Methods

Presented by: Dr. S. Sarpal

Background

- Term given to a mathematical algorithm OR a set of known sequences.
- Mixed with message to hide the meaning of content.
- Needed for personal privacy or security applications.
- Many analogue and digital encryption methods available.
- Earliest Ciphers – Vedic scriptures, the Egyptians, Julius Caesar ….
- Infamous example: Military communications (Enigma).

Cryptographic Jargon

- Crypto system.
- Plaintext (data to be encrypted).
- Ciphertext (encrypted data).
- Key.
- Alice, Bob, Carol and Dave.
- Eve (the eavesdropper!)

Types of analogue crypto systems

- Spectrum inversion:
  - AM modulation concept (inverted lower sideband)
  - Variable split band (VSB) and rolling codes used for greater security.
- Spectrum shift (AM concept, upper sideband).
- Cut and rotate (much more effective!)

General comments :

- Cheap to implement, does not require specialised hardware but offers limited security.
- Encrypted speech is discenable in some configurations.

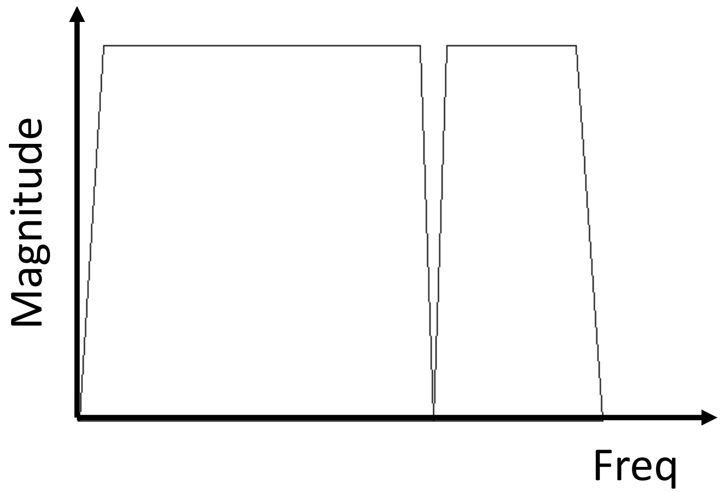
Spectrum Inversion Example

Using trigonometric identities…

$$\cos(w_c t).\cos(w_1 t) = \frac{1}{2}\cos(w_c - w_1) + \frac{1}{2}\cos(w_c + w_1)$$

- Analogue multiplier used.
- Hilbert transform can be used to remove upper sideband (DSP or computer implementation).

Audio VSB Spectrum Inversion Example



- Rolling code used to determine split point frequency (VSB).
- Split point frequency updated every 500ms.

- Original
- Encrypted

- Increased security than single carrier frequency.
- Low cost ASIC implementation available.

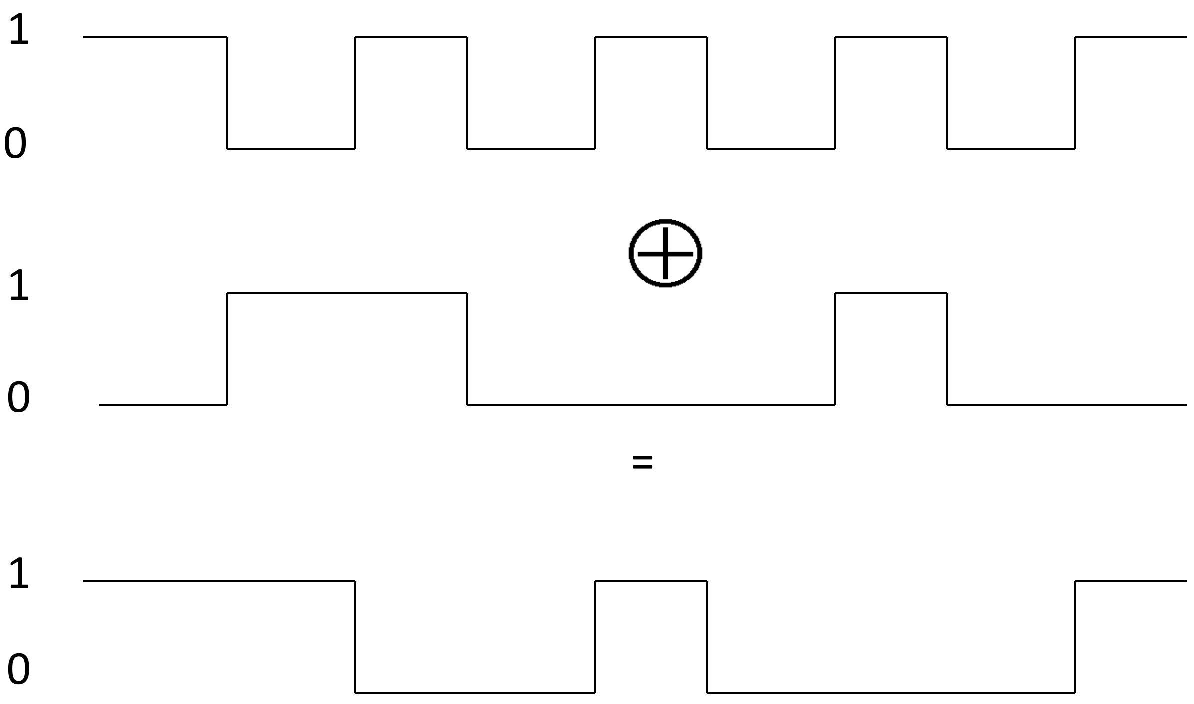
Types of digital crypto systems

- Symmetric (or secret key) encryption:
  - Same key used for encryption and decryption.
  - Fast operation on computer, DSP or micro-controller.
  - Examples: PRBS, DES, triple DES, RC2, IDEA, Blowfish, CAST-128, Skipjack, AES…
- Asymmetric (or public key) encryption:
  - Different keys for encryption and decryption.
  - Slow operation, best suited to a DSP or ASIC.
  - Examples: PGP, RSA, Diffie-Hellman, DSA, Elgamal …

General comments:

- Usually more expensive to implement than analogue methods.
- High level of security at much greater computation expense.

Simple digital encryption (PRBS)



$\oplus =$

A	B	Q
0	0	0
0	1	1
1	0	1
1	1	0

Asymmetric encryption (the RSA algorithm)

- Introduced in 1977.
- Named after its creators – Rivest, Shamir and Adleman.
- Used for secure encryption and digital signatures.
- Patented in 1983, but released into the public domain in September 2000.
- Commonly used – PGP, SSH, SSL, SET (Visa, Mastercard).
- Gets its security from the difficulty of factorizing large numbers.
- 1024-bit key is considered as the smallest key for secure communication.
- Many references have demonstrated that 300-bit or shorter keys can be broken in few hours using a simple laptop and freely available software!

Overview of the RSA algorithm
Key Generation

- Two random large prime numbers, **p** and **q** are chosen. For maximum security, **p** and **q** should be of equal length.
- Calculate product **n=p × q**
- Calculate random encryption key, **e** such that **e** and **(p-1) × (q-1)** are relatively prime.
- Finally, extended Euclidean algorithm is used for computing the decryption key **d**, such that:

$$e \times d = 1 \bmod (p-1) \times (q-1)$$

PUBLIC KEY: e, n

PRIVATE KEY: d

Overview of the RSA algorithm
Encryption/decryption

Encryption

To encrypt our plaintext message **m** using our public key, **e**:

$$\mathbf{c = m^e \bmod n}$$

Example: m = 123, p = 29, q = 31, e = 13, d = 517

$$c = 123^{13} \pmod{[29 \times 31]} = 402$$

Decryption

To decrypt the ciphertext **c** using our private key, **d**:

$$\mathbf{m = c^d \bmod n}$$

$$m = 402^{517} \pmod{[29 \times 31]} = 123$$

Thank you for your attention, please feel free to ask any questions.