Synchronous stream cipher

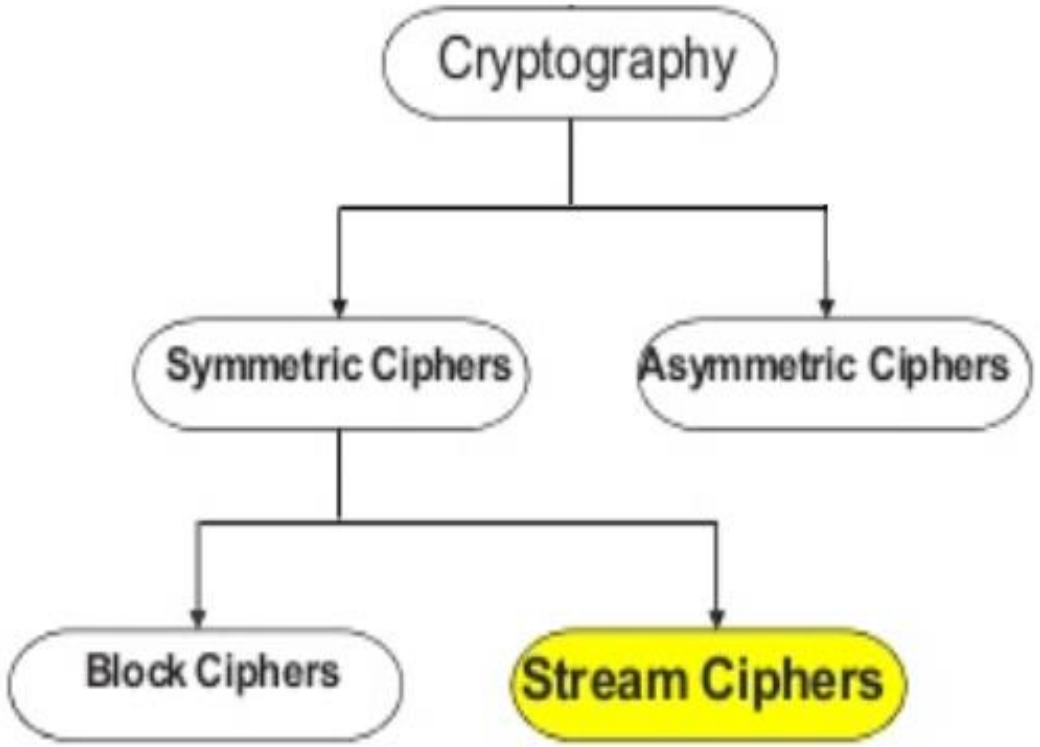
Updates

- Paper publishing update (Lead, Investigators, Writers)
  - Choon Kiat – Dianshi, Su, Leong
  - Eugene – Nidhya, Anila, Sharon
  - Hoe Fong – Peng Kiat, Herman, William, Jun wei
- Self proposed projects
  - Initial proposal : 19 Mar
  - Final : 2-Apr
- LAUNCHSomething
  - 3 days Startup seminar
  - Any idea?

Ciphers

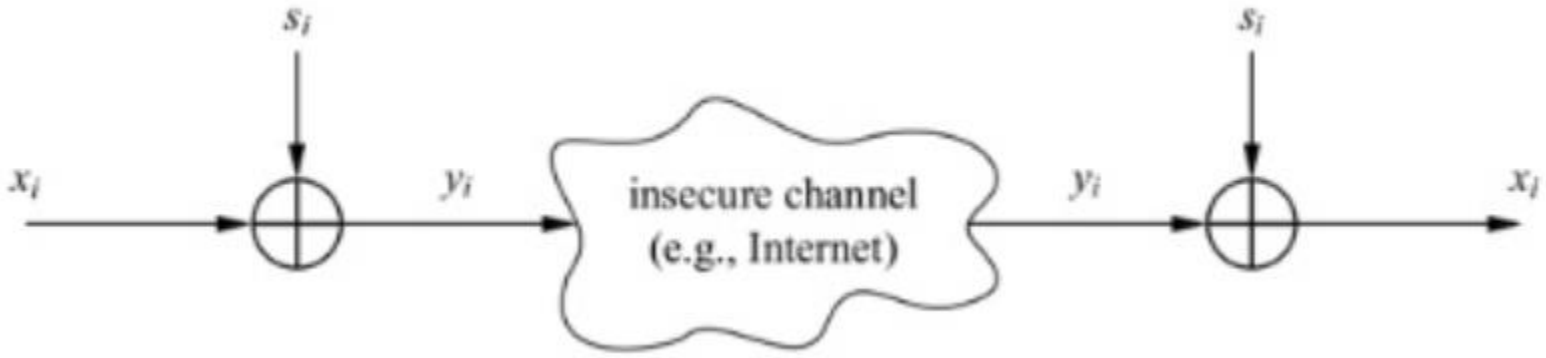
- Which type is AES & RSA & OTP?
- Stream ciphers invented by Vernam
  - Encrypts bits individually
  - Fast
  - Used in embedded devices
  - Vulnerable to attacks if key reused
- Block ciphers started with DES
  - Encrypts a full block (several bits)
  - Used in Internet applications

Cipher	Key length	Mbit/s
DES	56	36.95
3DES	112	13.32
AES	128	51.19
RC4 (stream cipher)	(choosable)	211.34



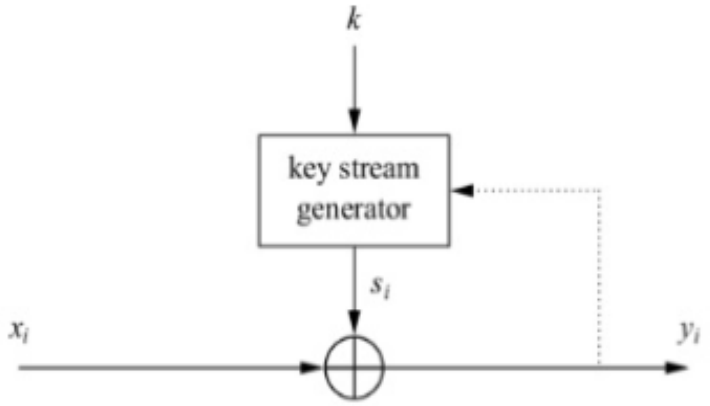
Stream Ciphers

- Plaintext, keystream , ciphertext



x_i	s_i	y_i
0	0	0
0	1	1
1	0	1
1	1	0

- Encryption and decryption are simple XORs (aka additions modulo 2)
- Security depends entirely on the keystream
  - Must be random and reproducible by sender & receiver
  - Keystream depends on the seed k



Dotted line is for async stream cipher where there's feedback