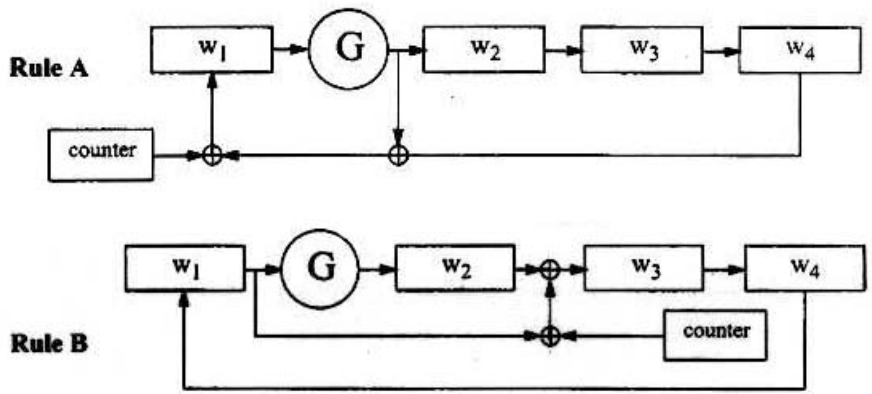
SKIPJACK and Key Exchange Algorithm (KEA)

Carlton J. O’Riley

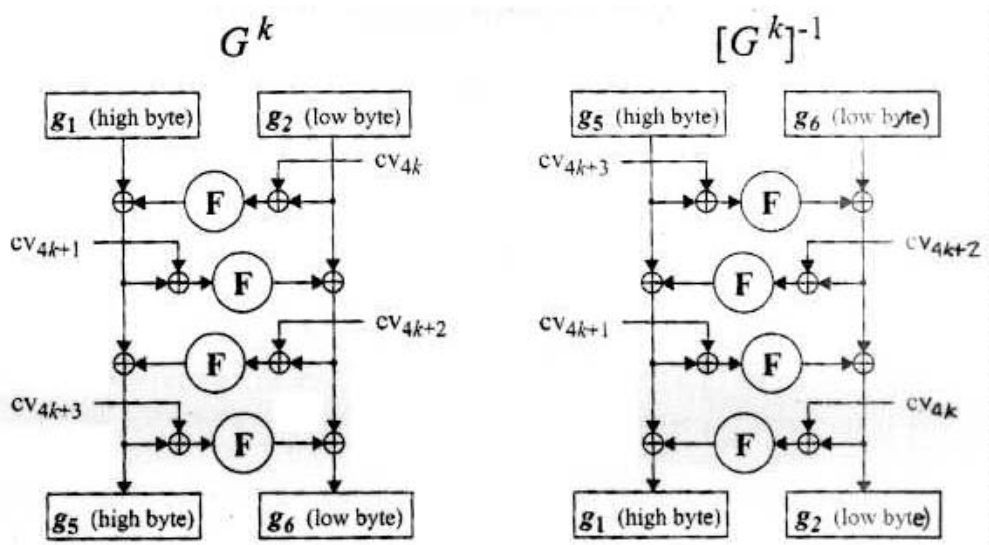
SKIPJACK Algorithm

- 64-bit Input/Output
- 80-bit Cryptovariable (Key)
- 32 Rounds
  - 8 Rounds of Rule A
  - 8 Rounds of Rule B
  - 8 Rounds of Rule A
  - 8 Rounds of Rule B



SKIPJACK Algorithm (Cont'd)

- G Permutation Function
  - 4 Round Feistel Structure
- F Byte Substitution Table



SKIPJACK Optimizations

- Precomputation of F-Table Key Values

  F(Key[0][0..255])

  …

  F(Key[9][0…255])

- Requires 2560 bytes of a lookup table, but saves 4 XORs per round

SKIPJACK Optimizations (Cont'd)

- Not Shifting Words, But Operands
- Inline G Functions (not subroutines)
- Pointers To Buffer Data
- Compiler Optimizations

SKIPJACK Optimizations (Cont'd)

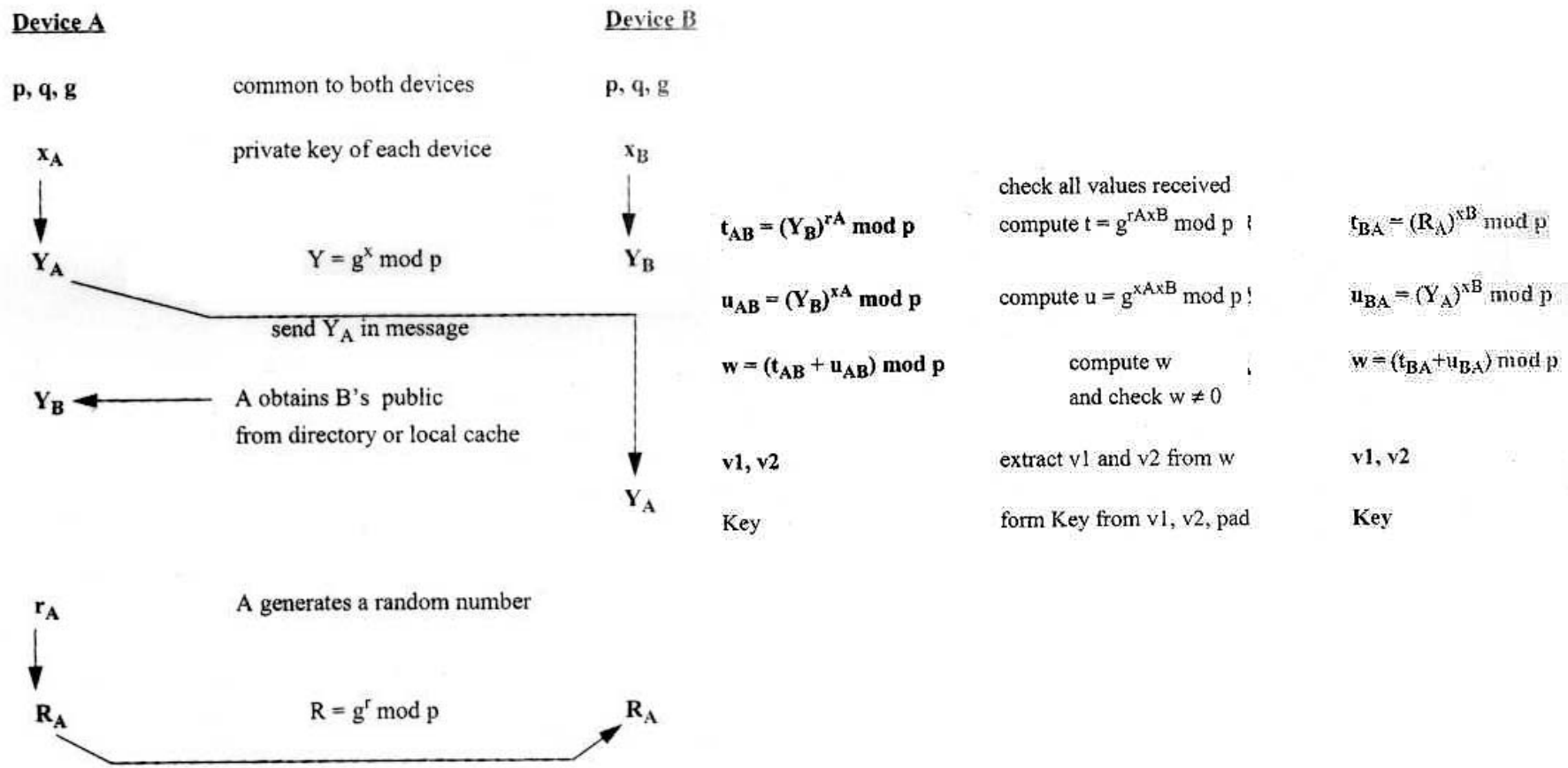
	Encryption	Decryption
SKIPJACK	34 ms	29 ms
DES	16 ms	16 ms

Key Exchange Algorithm

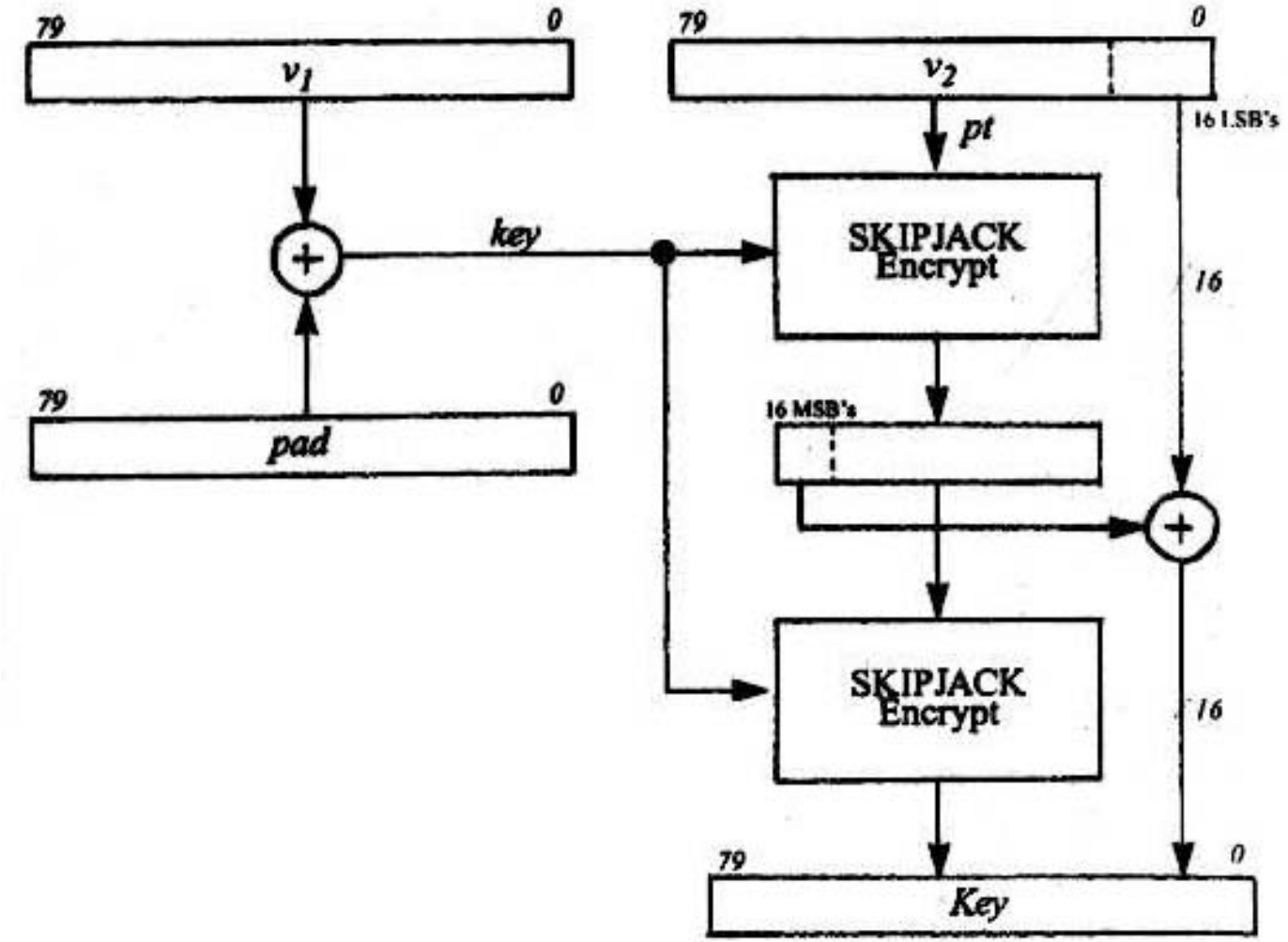
KEA Parameters

- Common Network Parameters
  - p : 1024-bit prime number
  - q : 160-bit prime divisor of p-1
  - g : 1024-bit base for exponentiation
- x : 160-bit Private Keys
- Y : 1024-bit Public Key (based on x)
- r : 160-bit Private Random Number
- R : 1024-bit Public Random Number (based on r)

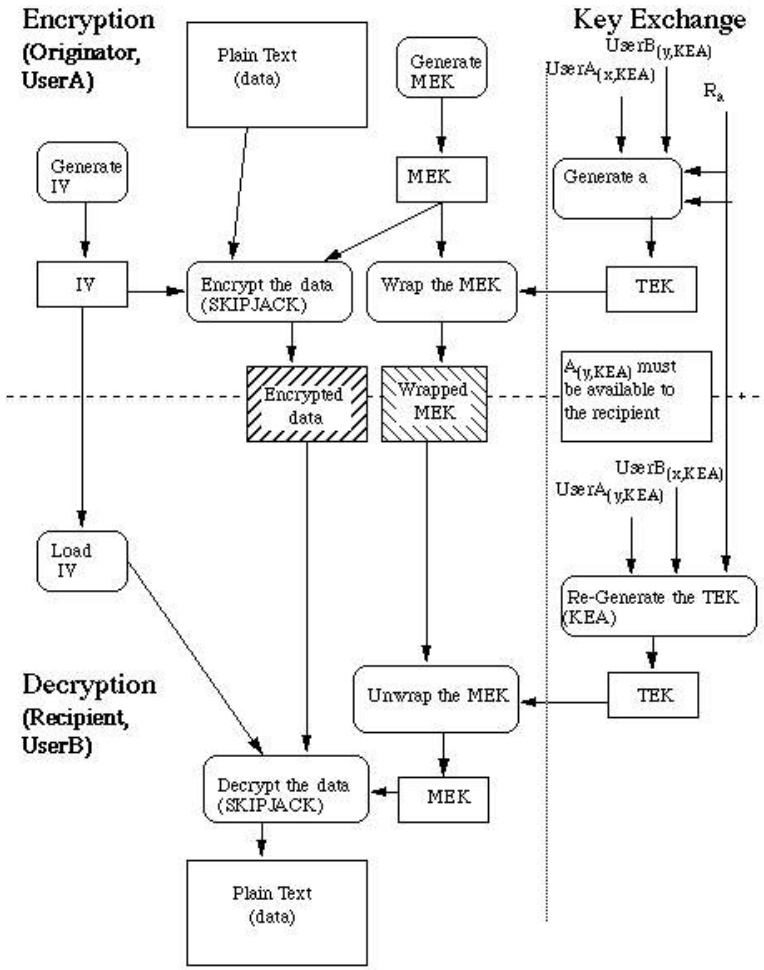
Store and Forward KEA (Cont'd)



KEA Key Generation



FORTEZZA KEA



Wrapping the MEK

- Pad 80-bit MEK With Six Bytes of 06
- Encrypt Each 64-bits Using SKIPJACK With TEK As Key