

1.(12pts) Choose "TRUE" or "FALSE."

- The Skipjack algorithm is a Feistel network. FALSE ****
- The Blowfish cipher is a slightly modified Feistel network. TRUE *****
- The round function of the Skipjack algorithm is a Feistel network. TRUE *****
- The RC4 cipher has variable key length. TRUE *****
- The Skipjack key schedule is straightforward: It consists in cyclically repeating the key enough times to fill the key schedule buffer; no other operations are performed. TRUE ****
- Skipjack supports variable key lengths. FALSE *****

2.(30 pts) Fill in the blanks.

- Double encryption does not provide enough security to justify the extra computational effort, because of the man-in-the-middle ***** attack, which uses a few known plaintext-ciphertext pairs and recovers the key in just twice as many tries as it would take for exhaustive key search in the single-encryption case.
- RC4 is a stream ***** cipher, operating byte-by-byte on the plaintext input.
- The internal state of RC4 is a permutation ***** of all 256 possible byte values.
- DES has effective key length of 56 bits, and the effective key length of 3-DES with two keys is 112 ***** bits.
- The Blowfish round function is designed to make cryptanalysis more difficult by mixing XOR with addition ***** mod 32.
- The Blowfish key schedule has several stages. First, the P -array and the S -boxes are filled with the binary-expansion of the fractional part of the number π *****. Then the key ***** is cyclically extended and XORED with the P -array and S -boxes. Finally, the values of the P -array and S -boxes are incrementally substituted by applications of Blowfish ***** encryption.
- The simplicity of Skipjack's key schedule algorithm results in an algorithm with good key agility ***** characteristics, meaning it supports dynamic key changes in a constrained computational setting.
- The RC4 cipher has two algorithms, a key-scheduling algorithm, and an algorithm for generation of pseudo-random ***** bytes.

3. (8 pts) List the numbers:

- The key length of Skipjack: 80 bits *****.
- The number of rounds of Blowfish: 16 *****.
- The size of the internal-state buffer of RC4: 256 bytes *****.
- The block size of 3-DES: 64 bits. *****.