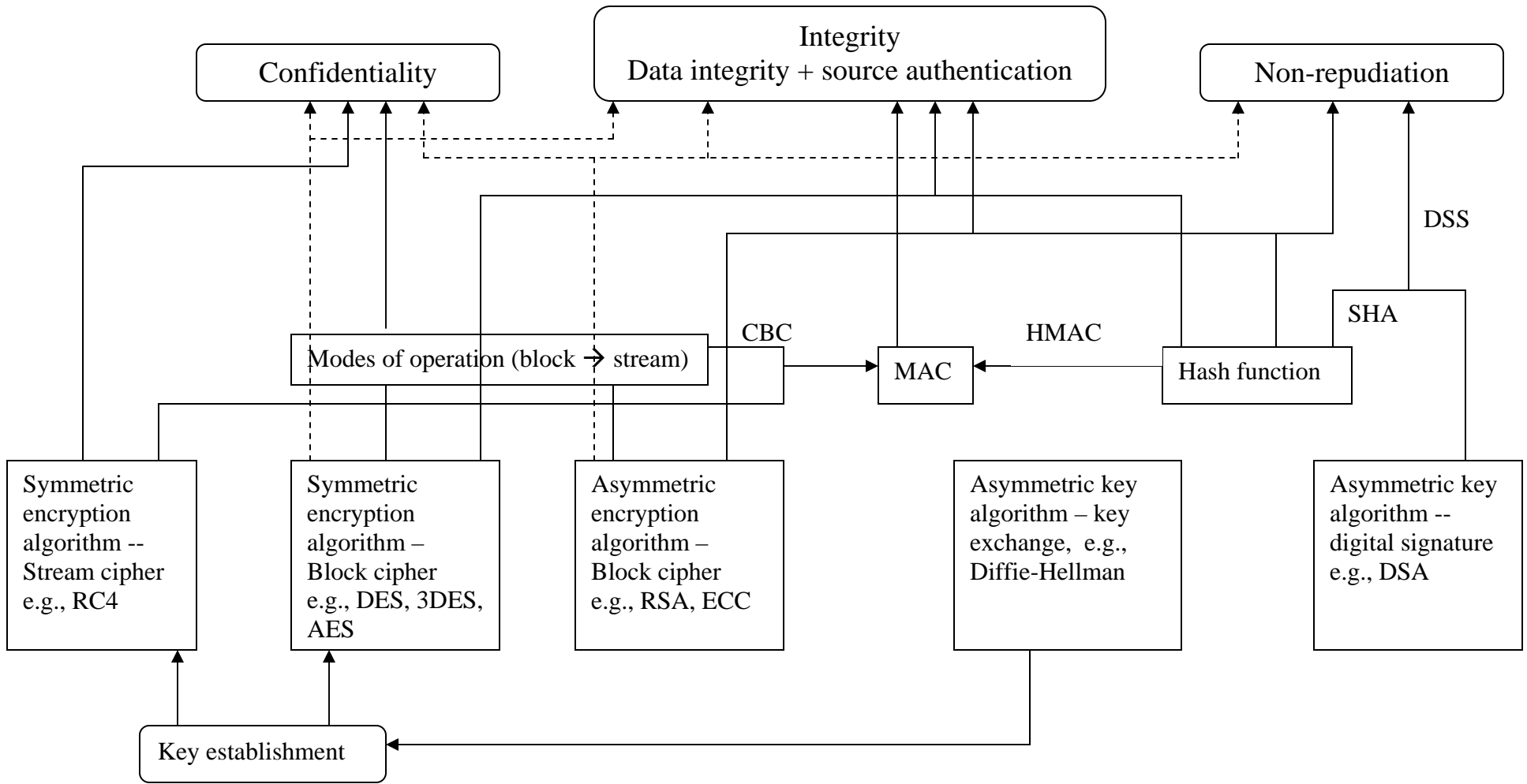


Category	Symmetric key algorithm					Asymmetric key algorithm					Hash function	
Algorithm	DES	3DES	Blowfish	AES	RC4	Encryption/Decryption; Digital Signature; Key-Exchange			Key-Exchange	Digital Signature	MD5	SHA-1
						RSA	ECC	ElGamal	Diffie-Hellman	DSA		
Block/Stream	B (64 bits)	B (64 bits)	B (64 bits)	B (128 bits)	Stream	B (n=1024)	B	B	N/A	N/A	S	S
Design principle	Feistel network.	Feistel network.	Feistel network.	substitution-permutation network; finite field	pseudo-random generation	Factoring problem; modular exponent	Discrete logarithm problem	discrete logarithm problem (based on Diffie-Hellman)	Discrete log	Elgamal signature		
Security	Key: 56 bits; Considered insecure now	Key: 168 bits (112 bits effective); man-in-the middle attack	128-bit no effective cryptanalysis	Key: 128-bit, 192-bit, 256-bit	Key: 128 bit, Needs careful key generation	n=1024			man in the middle attack		Digest length = 128 bits; Considered vulnerable.	Digest length = 160 bits;
comment	Developed by IBM; adopted by NBS in 1976; no longer recommended	Developed by IBM in 1978; Slow	1993 by Bruce Schneier; unpatented	Developed by Daemen and Rijmen; adopted by NIST in 2001	Developed by Rivest in 1987; used in SSL, WEP	1977 by Rivest, Shamir Adleman	Smaller keys and faster, compared with RSA	Elgamal in 1984; Used in GnuPG	1976 by Diffie and Hellman	By NIST in 1991	1991 by Rivest to replace MD4	1993 by NIST

* The shaded algorithms are covered in the lecture. Other algorithms are recommended for reading.



-----> Limited support for a block of data
 -----> Variable length message