The following notation is taken from the course textbook [1].

Symbol	*Expression*	*Meaning*
D, K	$\mathrm{D}(K, Y)$	Symmetric decryption of ciphertext Y using secret key K
D, PR_a	$\mathrm{D}(PR_a, Y)$	Asymmetric decryption of ciphertext Y using A's private key PR_a
D, PU_a	$\mathrm{D}(PU_a, Y)$	Asymmetric decryption of ciphertext Y using A's public key PU_a
E, K	$\mathrm{E}(K, X)$	Symmetric encryption of plaintext X using secret key K
E, PR_a	$\mathrm{E}(PR_a, X)$	Asymmetric encryption of plaintext X using A's private key PR_a
E, PU_a	$\mathrm{E}(PU_a, X)$	Asymmetric encryption of plaintext X using A's public key PU_a
K		Secret key
PR_a		Private key of user A
PU_a		Public key of user A
MAC, K	$\mathrm{MAC}(K, X)$	Message authentication code of message X using secret key K
$\mathrm{GF}(p)$		The finite field of order p, where p is prime. The field is defined as the set Z_p together with the arithmetic operations modulo p.
$\mathrm{GF}(2^n)$		The finite field of order 2^n
Z_n		Set of nonnegative integers less than n
gcd	$\gcd(i, j)$	Greatest common divisor; the largest positive integer that divides both i and j with no remainder on division.
mod	$a \bmod m$	Remainder after division of a by m
$\mathrm{mod}, \equiv$	$a \equiv b \pmod{m}$	$a \bmod m = b \bmod m$
$\mathrm{mod}, \not\equiv$	$a \not\equiv b \pmod{m}$	$a \bmod m \neq b \bmod m$
dlog	$\mathrm{dlog}_{a,p}(b)$	Discrete logarithm of the number b for the base $a \pmod{p}$
φ	$\phi(n)$	The number of positive integers less than n and relatively prime to n. This is Euler's totient function.
$\sum$	$\sum_{i=1}^{n} a_i$	$a_1 + a_2 + \cdots + a_n$
$\prod$	$\prod_{i=1}^{n} a_i$	$a_1 \times a_2 \times \cdots \times a_n$
$\vert$	$i \vert j$	i divides j, which means that there is no remainder when j is divided by i
$\vert, \vert$	$\vert a \vert$	Absolute value of a
$\Vert$	$x \Vert y$	x concatenated with y
$\approx$	$x \approx y$	x is approxiamtely equal to y
$\lfloor, \rfloor$	$\lfloor x \rfloor$	The largest integer less than or equal to x
$\in$	$x \in \mathbf{S}$	The element x is contained in the set $\mathbf{S}$

3DES	Triple DES; symmetric block cipher
AES	Advanced Encryption Standard; symmetric block cipher
CBC	Cipher Block Chaining mode of operation
CFB	Cipher Feedback mode of operation
CTR	Counter mode of operation
DES	Data Encryption Standard; symmetric clock cipher
ECB	Electronic Code Book mode of operation
FIPS	Federal Information Processing Standard
gcd	greatest common divisor
HTTPS	HTTP Security extensions
IP	Internet Protocol; network layer
IPsec	IP Security protocol; network layer
LAN	Local Area Network
MAC	Message Authentication Code
OFB	Output Feedback mode of operation
OSI	Open Systems Interconnection architecture
PGP	Pretty Good Privacy
PRF	Pseudo Random Function
PRNG	Pseudo Random Number Generator
RC4	stream cipher
RSA	Rivest-Shamir-Adleman algorithm
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer; transport layer
TRNG	True Random Number Generator
XOR	Exclusive OR

References

[1] W. Stallings. *Cryptography and Network Security: Principles and Practice.* Prentice Hall, fifth edition, 2011.