☆	J. DAEMEN AND V. RIJMEN. The Design of Rijndael.AES - The Advanced Encryption Standard. Springer, 2002.	배성호	1	PT #1
★	M. E. HELLMAN. A cryptanalytic time-memory trade-off. IEEE Transactions of Information Theory, 26 (1980), 401-406.	임준현	2	
☆	E. BIHAM AND A. SHAMIR. Differential cryptanalysis of the full 16-round DES. LNCS 740 (1993), 494-502. (CRYPTO '92)	장래영	3	
☆	M. BELLARE AND P. ROGAWAY. Optimal asymmetric encryption. Lecture Notes in Computer Science, 950 (1995), 92-111. (EUROCRYPT '94)	조준희	4	
☆	S. GOLDWASSER AND S. MICALI. Probabilistic encryption. Journal of Computer and Systems Science, 28 (1984), 270-299.	황대성	5	
★	J. H. Moore. Protocol failures in cryptosystems. In Contemporary Cryptology, The Science of Information Integrity, pages 541-558. IEEE Press, 1992.	남궁호	6	PT#2
☆	M. BELLARE, J. KILIAN AND P. ROGAWAY. The security of the cipher block chaining message authentication code. Journal of Computer and System Sciences, 61 (2000), 362-399.	장래영	7	
★	W. DIFFIE AND M. E. HELLMAN. New directions in cryptography. IEEE Transactions on Information Theory, 22 (1976), 644-654.	조준희	8	
★	M. MATSUI. Linear cryptanalysis method for DES cipher. LNCS 765 (1994), 386-397. (EUROCRYPT '93)	배성호	9	
☆	M. BELLARE AND P. ROGAWAY. Random oracles are practical: a paradigm for designing efficient protocols. In First ACM Conference on Computer and Communications Security, pages 62-73. ACM Press, 1993.	김영삼	10	
☆	N. T. COURTOIS AND J. PIEPRZYK. Cryptanalysis of block ciphers with overdefined systems of equations. LNCS 2501 (2002), 267-287. (ASIACRYPT 2002)	조준희	11	PT#3
☆	S. C. POHLIG AND M. E. HELLMAN. An improved algorithm for computing logarithms ove GF(p) and its cryptographic significance. IEEE Transations on Information Theory, 24 (1978), 106-110.	황대성	12	
☆	M. J. WIENER. Cryptanalysis of short RSA secret exponents. IEEE Transations on Inforamtion Theory, 36 (1990), 553-558.	남궁호	13	
★	T. ELGAMAL. Apublic key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31 (1985), 469-472.	장래영	14	
☆	D. CHAUM AND H. VAN ANTWERPEN. Undeniable signature. LNCS 435 (1990), 212-216. (CRYPTO '89)	신지강	15	
☆☆	P. BEAUCHEMIN AND G. BRASSARD, C. CREPEAU, C. GOUTIER and C. POMERANCE. The generation of random numbers that are probably prime. Journal of Cryptology, 1 (1988), 53-64.	남궁호	16	PT#4
☆☆	M. BELLARE AND P. ROGAWAY. The exact security of digital signatures: how to sign with RSA and Rabin. LNCS, 1070(1996), 399-416. (EUROCRYPT '96)	임준현	17	
★	A. FIAT AND A. SHAMIR. How to prove yourself: practical solutions to identification and signature problems. LNCS 263 (1987), 186-194. (CRYPTO '86)	김영삼	18	
☆☆	M. BELLARE. Practice-oriented provable-security. In Lectures on Data Security, pages 1-15. Springer, 1999.	신지강	19	
★	A. FIAT AND M. NAOR. Broadcast encryption. LNCS 773 (1994), 480-491. (CRYPTO '93)	황대성	20	
☆	M. BURMESTER AND Y. DESMEDT. A secure and efficient conference key distribution system. LNCS 250 (1994), 275-286 (EUROCRYPT '94)	김영삼	21	PT#5
★	U. FEIGE, A. FIAT AND A. SHAMIR. Zero-knolwedge proofs of identity. Journal of Cyrptology, 1 (1988), 77-94	신지강	22	
☆	C. P. SHNORR. Efficient signature generation by smart cards. Journal of Cryptology, 4 (1991), 161-174.	임준현	23	
☆	D. E. DENNING AND G. M. SACCO. Timestamps in key distribution protocols. Communications of the ACM 24 (1981), 533-536.	배성호	24	

★ : 필수, ☆: 난이도 1, ☆☆: 난이도 2(가산점)