DAFTAR PUSTAKA

Backes, Michael dan Pfitzmann, Birgit, 2004, A Cryptographically Sound Security Proof of the Needham-Schroeder-Lowe Public-Key Protocol, *IEEE Journal on Selected Areas in Communications*, 22, 2075-2086.

Cormen, T. H., Leiserson, C. E., Rivest, R. L., dan Stein, C., 2009, *Introduction to Algorithm*, 3rd, The MIT Press, London.

Daubignard, Marion, Lubicz, David dan Steel, Graham, 2014, A Secure Key Management Interface with Asymmetric Cryptography, *POST*, 63-82.

Diffie, W. dan Hellman, M. E., 1976, New Directions in Cryptography, *IEEE Transaction on Information Theory*, 6, IT-22, 644-654.

Dolev, D., Even, S., dan Karp, R. M., 1982, On the Security of Ping-Pong Protocols, *Information and Control*, 55, 57-68.

Dolev, Danny dan Yao, Andrew C., 1983, On the Security of Public Key Protocol, *IEEE Transactions on Information Theory*, 2, IT-29, 198-208.

Halim, Steven dan Halim, Felix, 2011, *Competitive Programming*, 2nd, Lulu, North Carolina.

Hopcroft, J. E., Motwani, R., dan Ullman, J. D., 2006, *Introduction to Automata Theory, Languages, and Computation*, 3rd, Pearson, New York.

Lowe, Gavin, 1995, An Attack on the Needham-Schroeder Public-Key Authentication Protocol, *Information Processing Letters*, 56, 131-133.

Lowe, Gavin, 1996, Breaking and Fixing the Needham-Schroeder Public-Key Protocol Using FDR, *Proceedings of the Second International Workshop on Tools and Algorithms for Construction and Analysis of Systems*, 147-166.

Needham, Roger M. dan Schroeder, Michael D., 1978, Using Encryption for Authetication in Large Network of Computers, *Communications of The ACM*, 12, 21, 993-999.

Rivest, R. L., Shamir, A., dan Adleman, L., 1978, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of The ACM*, 21, 120-126.

Stallings, William, 2011, *Cryptography and Network Security*, 5th, Pearson, New York.