traditional names for roles in cryptography

Canonical name	TraditionalNamesForRolesInCryptography
Date of creation	2013-03-22 15:13:41
Last modified on	2013-03-22 15:13:41
Owner	lieven (1075)
Last modified by	lieven (1075)
Numerical id	6
Author	lieven (1075)
Entry type	Definition
Classification	msc 94A60

In the field of cryptography, protocols are described and analysed to allow a number of parties to achieve certain goals like communication, authentication, voting etc. Initially these protocol descriptions used single letter variables in the style “Let A and B be parties trying to communicate with the help of a mutually trusted entity C.”. This gave rise to a lot of repetition so a sort of pseudo-standard has arisen that uses first names for some of the standard roles. Common are Alice and Bob as the first two parties in a protocol. If more parties are needed, the following ones are Carol and Dave. Eve is a passive attacker, an eavesdropper. Mallory is an active attacker. Trent is a trusted third party like a mutually known key server. In the field of prove carrying code, there’s Peggy the prover and Victor the verifier. The list at wikipedia (http://en.wikipedia.org/wiki/Characters_in_cryptography) contains even more elements from this bestiary.