Alice and Bob

Make a donation *to Wikipedia and give the gift of knowledge!*

From Wikipedia, the free encyclopedia

The names **Alice and Bob** are commonly used placeholders for archetypal characters in fields such as cryptography and physics. The names are used for convenience, since explanations such as "Person *A* wants to send a message to person *B*" can be difficult to follow in complex systems involving many steps. Following the alphabet, the specific names have evolved into common parlance within these fields — helping technical topics to be explained in a more understandable fashion.

In cryptography and computer security, there are a number of widely-used names for the participants in discussions and presentations about various protocols. The names are conventional, somewhat self-suggestive, sometimes humorous, and effectively act as metasyntactic variables.

In typical implementations of these protocols, it is understood that the actions attributed to characters such as Alice or Bob would not normally be carried out by human parties directly, but rather by a trusted automated agent (such as a computer program) on their behalf.

Contents

List of characters

This list is drawn mostly from the book *Applied Cryptography* by Bruce Schneier. Alice and Bob are archetypes in cryptography; Eve is also common. Names further down the alphabet are less common.

- **Alice** and **Bob**. Generally, Alice wants to send a message to Bob. These names were used by Ron Rivest in the 1978 *Communications of the ACM* article presenting the RSA cryptosystem, and in *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* published April 4, 1977, revised September 1, 1977 as technical Memo LCS/TM82. Rivest denies that these names have any relation to the 1969 movie *Bob & Carol & Ted & Alice* as occasionally suggested by others.
- **Carol** or **Charlie**, as a third participant in communications.
- **Dave**, a fourth participant, and so on alphabetically.
- **Eve**, an *eavesdropper*, is usually a passive attacker. While she can listen in on messages between Alice and Bob, she cannot modify them. In quantum cryptography, Eve may also represent the *environment*.
- **Isaac**, an Internet Service Provider (ISP).
- **Ivan**, an *issuer* (as in financial cryptography).
- **Justin**, from the *justice* system.
- **Mallory**, a *malicious attacker*; unlike Eve, Mallory can modify messages, substitute her own messages, replay old messages, and so on. The problem of securing a system against Mallory is much greater than against Eve. The names **Marvin** and **Mallet** can also be used for this role.
- **Matilda**, a *merchant* (as in e-commerce or financial cryptography).
- **Oscar**, an *opponent*, is usually taken as equivalent to Mallory.
- **Pat** or **Peggy**, a *prover*, and **Victor**, a *verifier*, often must interact in some way to show that the intended transaction has actually taken place. They are often found in zero-knowledge proofs. Another name pair sometimes used is **Pat** and **Vanna** (after the host and hostess on the *Wheel of Fortune* television show).
- **Plod**, a law enforcement officer (also "Officer Plod") from the children's fictional character Mr. Plod, in the *Noddy* books by Enid Blyton.
- **Steve**, sometimes used in reference to Steganography.
- **Trent**, a *trusted arbitrator*, is some kind of neutral third party, whose exact role varies with the protocol under discussion.
- **Trudy**, an intruder: another alternative to Mallory.
- **Walter**, a *warden*, may be needed to guard Alice and Bob in some respect, depending on the protocol being discussed.
- **Zoe**, often the last party to be involved in a cryptographic protocol.

Although an interactive proof system is not quite a cryptographic protocol, it is sufficiently related to mention the 'cast of characters' its literature features:

- **Arthur** and **Merlin**: In interactive proof systems, the prover has unbounded computational ability and is hence associated with Merlin, the powerful wizard. He claims the truth of a statement, and Arthur, the wise king, questions him to verify the claim. These two characters also give the name for two complexity classes, namely MA and AM.

See also

- Metasyntactic variable
- Dave and Sue

References

- C.H. Lindsey, Regulation of Investigatory Powers Bill: Some Scenarios, 2000, [1].

External links

- A Method for Obtaining Digital Signatures and Public-Key Cryptosystems
- The Alice and Bob After Dinner Speech
- Alice and Bob jokes (mainly Quantum Computing-related)
- Alice and Bob: IT's inseparable couple
- A short history of Bobs (story and slideshow) in the computing industry, from Alice & Bob to Microsoft Bob and Father of Ethernet Bob Metcalfe
- XKCD comic featuring Alice and Bob

Retrieved from "http://en.wikipedia.org/wiki/Alice_and_Bob"
Categories: Cryptographic protocols | Placeholder names
Hidden category: Articles with Alice and Bob explanations

- This page was last modified on 19 May 2008, at 20:00.
- All text is available under the terms of the GNU Free Documentation License. (See **Copyrights** for details.) Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a U.S. registered 501(c)(3) tax-deductible nonprofit charity.