Samuel Seidel

Dave Busse

IT Analysis and Design (41011)

4/23/2017

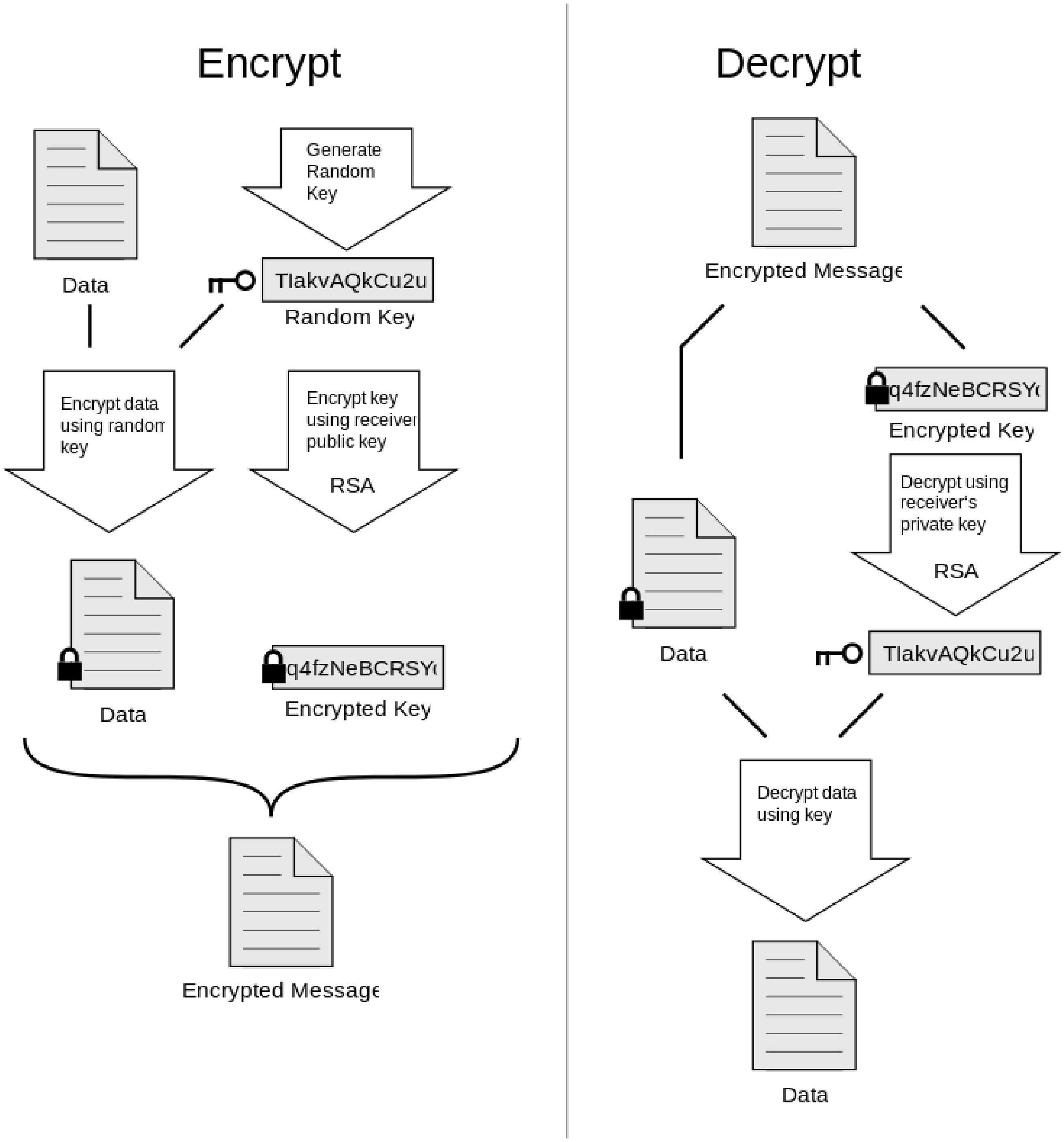
PGP

Pretty Good Privacy, abbreviated PGP, is an encryption program providing cryptographic privacy and authentication for data communications. PGP was developed by Philip R. Zimmermann, Jr in 1991. The software and it's source code was made available publicly through FTP for anyone to download. It became the first widely available program implementing public-key cryptography. It then became available overseas via the Internet, later causing an investigation over the United States *Arms Export Control Act*. The Unites States Government long considered cryptographic software as munition and therefore subject to arms trafficking export controls. The investigation lasted three years, but was finally dropped. Later, the boundaries on export laws were raised allowing PGP to be exported legally. Zimmerman later, in 1996, founded PGP Inc. and continued development of the software. The company was acquired by Network Associates (NAI) in December 1997, and Zimmerman stayed on the payroll for three years as a Senior Fellow. NAI dropped PGP in 2002 and the rights were acquired by a new company called PGP Corporation. Zimmerman continued to act as a special advisor and consultant to that firm until its demise, in 2010, through the acquisition, of the entire company, by Symantec.

Passphrase

A passphrase is a series of words or other text used to control access to a computer system, program or data.

How PGP Works: (Wikipedia, License: CC BY-SA 3.0)



When a user encrypts plaintext with PGP, PGP first compresses the plaintext. PGP then creates a session key, which is a single-use, secret key. The data is encrypted with the session key, and the session key is then encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the *session key encrypted data* to the recipient. Decryption works in the reverse. The recipient's copy of PGP uses his or her private key to recover the temporary session key, which PGP then uses to decrypt the *session key encrypted data*.
(https://users.ece.cmu.edu/~adrian/630-f04/PGP-intro.html#p10)

Sidenote: Philip also was a principal designer of the cryptographic key agreement protocol (the "association model") for the Wireless USB standard. Wireless USB has been dead for quite some time, however I happened to have bought one of the few implementations of WUSB doing its short lifespan.