Great Crypto & Info Security Quotes

"*The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated...*"
-- The Fourth Amendment to the U.S. Constitution

"*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.*"
-- The First Amendment to the U.S. Constitution

"*The freedom of speech and of the press guaranteed by the Constitution embraces at the least the liberty to discuss publicly and truthfully all matters of public concern without previous restraint or fear of subsequent punishment.*"
-- Roth v. United States, 354 U.S. 476 (1957)

"*...domestic intelligence activities [that] threaten to undermine our democratic society and fundamentally alter its nature*"
-- Senate Church Committee report, 1976

"*the debate over national cryptography policy can be carried out in a reasonable manner on an unclassified basis*"
-- A Congress requested National Research Council report "Cryptography's role in securing the information society", 1996

"*on balance, the advantages of more widespread use of cryptography outweigh the disadvantages*"
-- ibid

"*The FBI, on the other hand, stretched the truth and distorted the fact. It seems fair to conclude that the government has not made its case regarding encryption.*"
-- Diffie in "Privacy on the line", 1998 - explaining how intelligence agencies (mis)use wiretap statistics.

"*In total, therefore, the U.S. economy will lose between $35.16 and $95.92 billion over the next five years, as a consequence of current administration policy [on crypto].*"
-- Economic Strategy Institute report "Finding the Key", 1998

"*The right to be let alone is indeed the beginning of all freedom.*"
-- Supreme Court Justice William O. Douglas 1952, Public Utilities Commission vs. Pollak

"*The right to be left alone - the most comprehensive of rights, and the right most valued by civilized men.*"
-- Supreme Court Justice Louis Brandeis

"*There is no assurance, without scrutiny, that all keying material introduced during the chip programming is not already available to the NSA..... As long as the programming devices are controlled by the NSA, there is no way to prevent the NSA from routinely monitoring all SKIPJACK encrypted traffic. Moreover, compromise of the NSA keys, such as in the Walker case, could compromise the entire EES system.*"
-- NASA comments on EES, 1993. ok - branches of the government don't trust the NSA, but we should?

"*Just because you're paranoid doesn't mean some one isn't out to get you...*"
-- Unknown

"*The disk scrambler is of course like any other entity which can be put to good, or bad use (I could perhaps strangle someone with a stethoscope for example....)*"
-- AMAN, 6 July 1998

"*The law does not allow me to testify on any aspect of the National Security Agency, even to the Senate Intelligence Committee.*"
-- General Allen, Director of the NSA, 1975

"*You bastards!*"

-- guy@panix.com in response to the above General Allen quote :-)

"*There can be no greater good than the quest for peace, and no finer purpose than the preservation of freedom.*"
-- U.S. President Ronald Reagan

"*I know something about trust. I got my trust the old-fashioned way. I earned it.*"

--Bill Clinton, in Federal News Service, 28 October 1992. Hehehehe.

"*The strength of the Constitution lies entirely in the determination of each citizen to defend it. Only if every single citizen feels duty bound to do his share in this defense are the constitutional rights secure.*"
-- Albert Einstein

"*It is dangerous to be right when the government is wrong.*"
-- Voltaire

"*So far as we are concerned, there is no difference between an encrypted file and a locked suitcase*"
-- UK Customs and Excise official, August 98. Apart from the fact you can force a locked suitcase open :-)

"*If all the personal computers in the world - ~260 million computers - were put to work on a single PGP-encrypted message, it would still take an estimated 12 million times the age of the universe, on average, to break a single message.*"
-- William Crowell, Deputy Director of the National Security Agency, March 1997

"*Without censorship, things can get terribly confused in the public mind.*"
-- U.S. General William Westmoreland

"*I would rather be exposed to the inconveniences attending too much liberty than those attending too small a degree of it.*"
-- Thomas Jefferson

"*My comment was that the FBI is either incompetent or lying, or both.....*"
-- Bruce Schneier on FBI claims that they don't have specialised machines that can break DES

"*But I'd also ask American business not to make a campaign out of just trying to bust through export controls as though somehow there was a God-given, inherent right to send the strongest encryption to anybody in the world, no matter who they are. I don't agree with that. I will never agree with that.*"
-- Deputy Secretary of Defense John J. Hamre, 21 July, 1998. *But who said there is a god given right that the DoD can read my messages?*

"*You can torture me all you want, I don't know anything*"
"*torture you... that's a good idea*"
-- Resevoir Dogs (Quentin Tarantino)

"*The NSA response was, 'Well, that was interesting, but there aren't any ciphers like that.'*"
-- Gus Simmons - "The History of Subliminal Channels"

"*A secret between two is a secret of God; a secret among three is everybody's secret.*"
-- French proverb (about clipper / key-escrow systems? :-))

"*Can you say 'cryptographic filesystem'? Can you say 'custom filesystem'?*"
-- James MacDonald posting to sci.crypt, August 14, 1998. Sarcastic comment - made unwittingly to the author of ScramDisk :-)

"*The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers.*"
-- Bill Gates from The Road Ahead, p265

"*Cryptography is like literacy in the Dark Ages. Infinitely potent, for good and ill... yet basically an intellectual*

construct, an idea, which by its nature will resist efforts to restrict it to bureaucrats and others who deem only themselves worthy of such Privilege."
-- A Thinking Man's Creed for Crypto

"*There is a secret message embedded in the phosphor of this period.*"
-- David Honig [honig@sprynet.com] .sig

"*It's the dungheap of History. If you look really, really closely at the tippy top, you can see Louis Freeh holding a Clipper chip.*"
-- Xcott Craver posting to sci.crypt 20 August 1998. Describing the 'pyramid thing' on the cover of AC2 :-)

"*You shouldn't overestimate the I.Q. of crooks.*"
-- NYT: Stuart A. Baker, General Counsel for the NSA, explained why crooks and terrorists who are smart enough to use data encryption would be stupid enough to choose the U.S. Government's compromised data encryption standard.

"*An essential element of freedom is the right to privacy, a right that cannot be expected to stand against an unremitting technological attack.*"
-- Whitfield Diffie, Distinguished Engineer at Sun Microsystems

"*It must always be remembered that crime statistics are highly inflammatory---an explosive fuel that powers the nation's debate over a large number of important social issues---and that FBI Director Louis Freeh today is the leading official shovelling the fuel into the blazing firebox.*"
-- David Burnham

"*Why should you care if you have nothing to hide?*"
-- J. Edgar Hoover

"*I love my country but fear my government*"
-- Anonymous

"*...Finally, face it; PGP, albeit useful for some niche applications, is a little pissant pimple on the body of cryptographic usage.*"
-- David Sternlight posting to comp.security.pgp.discuss, June 25, 1997. Click here for more :-)

"*Where the hell is your great contribution to the field that I worked in?????*"
-- Robert Gifford posting to comp.security.pgp.discuss, Aug 25, 1999 to David Sternlight :-).

"*I have not got any father than just a few variables past one round. I tried to search for real info on the 3.5 rounds that some one reverseved engineered but could not find it.*"
-- The literate David A. Scott posting to sci.crypt , June 26, 1998. RE his analysis of IDEA :-)

"*I have developed an encryption software package that I can best describe as a ONE-TIME-PAD GENERATOR.*"
-- Anthony Stephen Szopa posting to sci.crypt, August 8, 1997

"*Is it time for another one of these already? Oh, bother.*"
-- Bruce Schneier posting to sci.crypt, August 8, 1997 - in response to the Szopa quote :-)

"*Quis Custodiet Ipsos Custodes.*" -> "*Who will watch the watchmen.*"
-- Juvenal, circa 128 AD

"*Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.*"
-- John Von Neumann, 1951

"*Random numbers should not be generated with a method chosen at random.*"
-- Donald Knuth, vol 2.

"*Key escrow to rule them all; key escrow to find them. Key escrow to bring them all and in the darkness bind them. In the land of surveillance where Big Brother lies.*"
-- Peter Gutmann

"*When cryptography is outlawed, bayl bhgynjf jvyy unir cevinpl.*"
-- Kevin McCurleys Thought for the day, June 24, 1997

"*Mary had a little key (It's all she could export),*
and all the email that she sent was opened at the Fort."
-- Ron Rivest

"*Mary had a crypto key, she kept it in escrow,*
and everything that Mary said, the Feds were sure to know."
-- Sam Simpson, July 9, 1998

"*There is a group at Fort Meade*
who fear that which they cannot read
so they fight with their friends
(God knows to what ends!)
In attempts to get more than they need."
-- Jim Bidzos, CEO of RSA Data Security

"*Feistel and Coppersmith rule. Sixteen rounds and one hell of an avalanche.*"
-- Stephan Eisvogel in de.comp.security, Jan 1998

"*The NSA regularly lies to people who ask it for advice on export control. They have no reason not to; accomplishing their goal by any legal means is fine by them. Lying by government employees is legal.*"
-- John Gilmore (gnu@toad.com)

"*In God we trust. Everybody else we verify using PGP!*"
-- Tim Newsome

"*BTW, I learned a lovely new acronym today: "Law Enforcement Agency Key" - LEAK.*"
-- Charles H. Lindsey (chl@clw.cs.man.ac.uk)

"*They that give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.*"
-- Benjamin Franklin

"*Necessity is the plea for every infringement of human freedom. It is the argument of tyrants; it is the creed of slaves.*"
-- William Pitt, British Prime Minister, November 18, 1783

"*There's no way to rule innocent men. The only power any government has is the power to crack down on criminals. Well, when there aren't enough criminals, one makes them. One declares so many things to be a crime that it becomes impossible to live without breaking laws.*"
-- Ayn Rand, "Atlas Shrugged"

"*This method, seemingly very clever, actually played into our hands! And so it often happens that an apparently ingenious idea is in fact a weakness which the scientific cryptographer seizes on for his solution.*"
-- Herbert Yardley, The American Black Chamber, p282, referring to a Japanese method of transposing the sections of a code message to hide the beginning and end.

"*I applied ROT13 to this, but that didn't make it any more intelligible!*"
-- Roger Schlafly posting to sci.crypt, 21st June 98 in response to a message posted in German :-)

"*The Internet treats censorship as a malfunction and routes around it.*"
-- John Perry Barlow

"*Liberty means responsibility. That is why most men dread it.*"
-- George Bernard Shaw

"*Furem fur cognoscit et lupum lupus. " -> "A thief recognises a thief and a wolf a wolf.*"
-- Anon

Taken from the ScramDisk user manual (http://www.hertreg.ac.uk/ss/)