Security

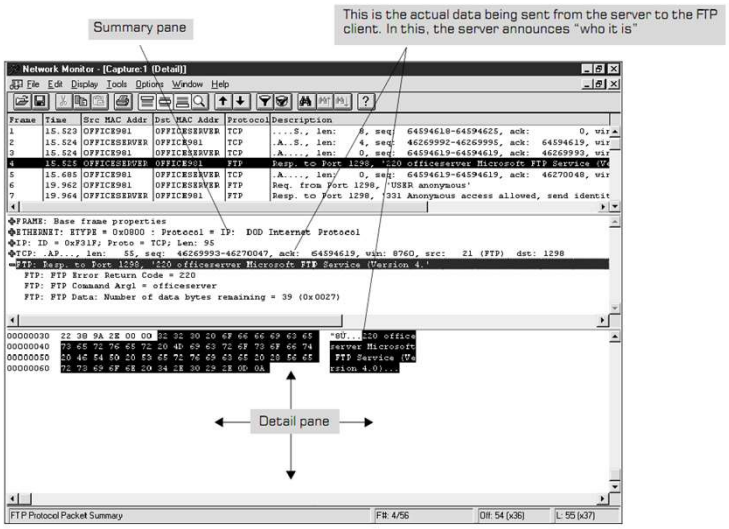
Aj.Drusawin Vongpramate
Information Technology
Science, BRU

The Need for Security

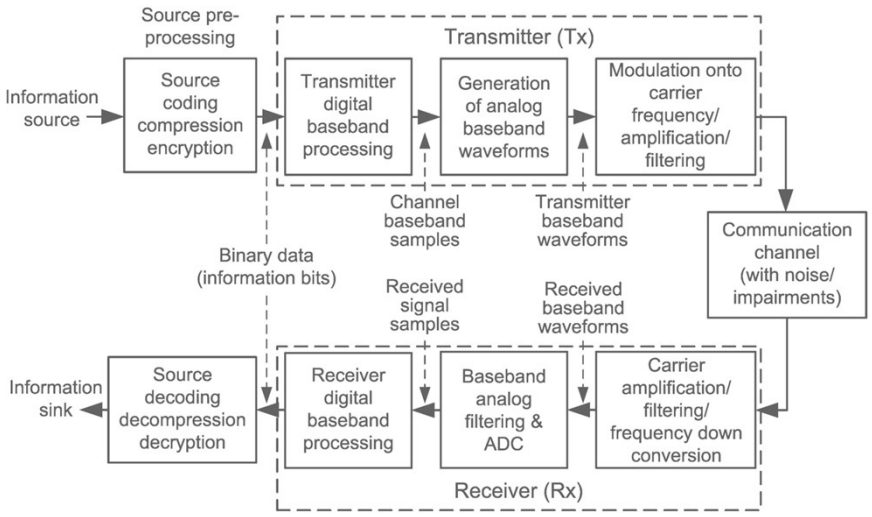
The Internet has, in many ways, become a victim of its own success. The Internet community now comprises many millions of people world-wide and as in any large community there are the "**good-guys**" and the "**bad-guys**".

REF: Keith Sutherland.2018.**Understanding the Internet A Clear Guide to Internet Technologies**, p77-96

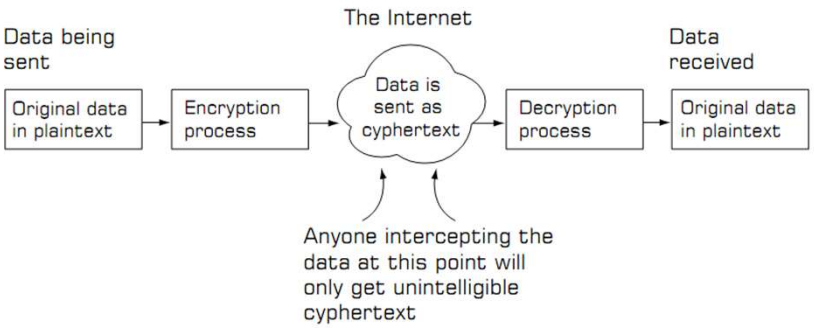
sniffer



Digital Communication System (CH3)



Protecting Data



Protecting Data

Most systems use a means of securing the data that can be divided into two parts. These are the **algorithm** (process) and the **key**.

Algorithms are the techniques used to conceal the patterns of data in a message.

The keys are patterns of binary digits that are fed into the algorithm together with the data to produce an unreadable and indecipherable output.

This output is often referred to as **cyphertext.**

Secret Algorithm

Caesar cipher

HELLO => **JGNNQ**

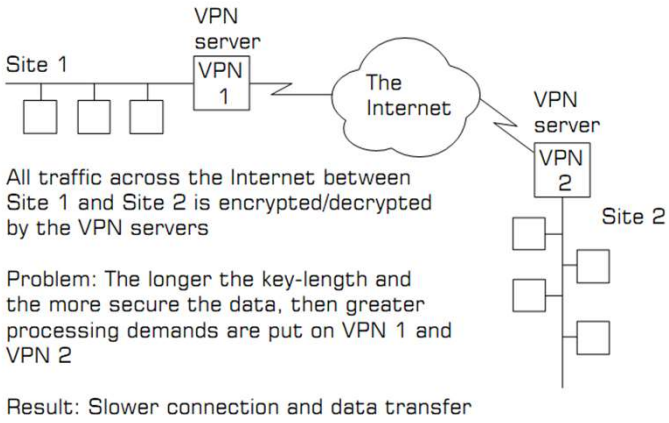
MD5

HELLO =>
c65f99f8c5376adadddc46d5cbcf5762f9e55eb7

Security Level	Work Factor	Algorithms
Weak	$O(2^{40})$	DES, MD5
Legacy	$O(2^{64})$	RC4, SHA-1
Baseline	$O(2^{80})$	3DES
Standard	$O(2^{128})$	AES-128, SHA-256
High	$O(2^{192})$	AES-192, SHA-384
Ultra	$O(2^{256})$	AES-256, SHA-512

1,099,511,627,776 possibilities.

Virtual Private Networks



All traffic across the Internet between Site 1 and Site 2 is encrypted/decrypted by the VPN servers

Problem: The longer the key-length and the more secure the data, then greater processing demands are put on VPN 1 and VPN 2

Result: Slower connection and data transfer

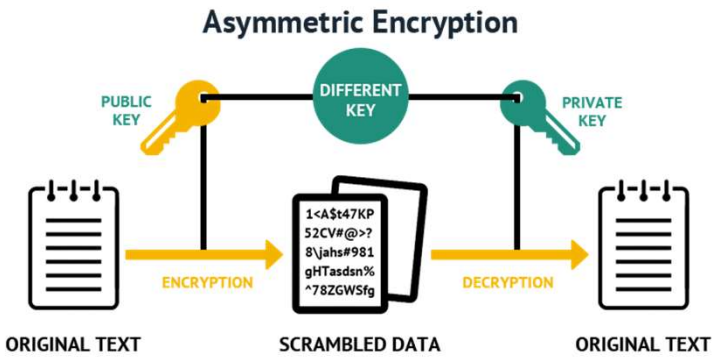
In such a VPN set-up **the keys used to encrypt and decrypt the data are the same**. This is referred to as **symmetric key encryption**.

Public–Private Keys

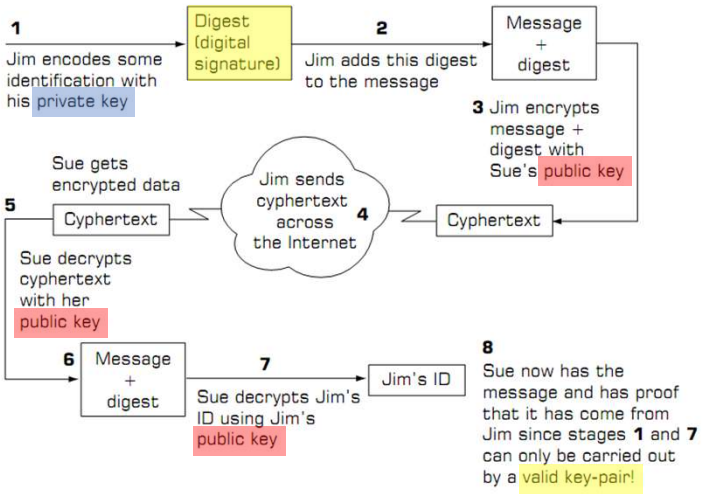
If we want to authenticate our clients, and we want to be able to prove our existence to prospective customers, then a more flexible and elegant solution is required.

The answer to this is in public key encryption (often referred to as **asymmetric key encryption**).

Public–Private Keys



Digital Signature



Other Solutions

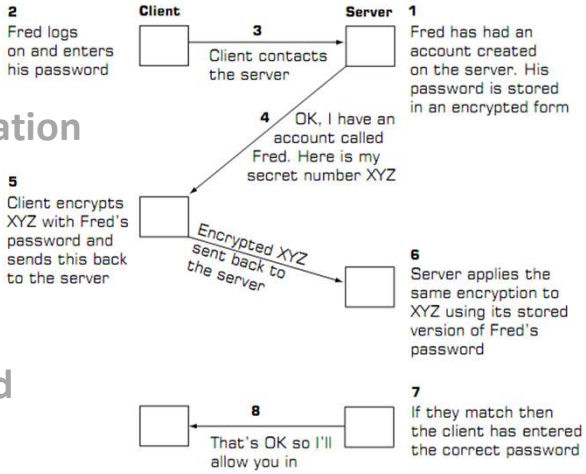
Most banks and other financial organisations use a combination of certification and an authenticating system called **challenge/response** to guarantee authentication. Once this has been done then a combination of public/private key encryption is used to protect the data.

https://www.techspot.com/news/77780-hacker-steal-millions-eastern-european-banks-sneaking-devices.html

Challenge/Response

P : Personal
I : Identification
N : Number

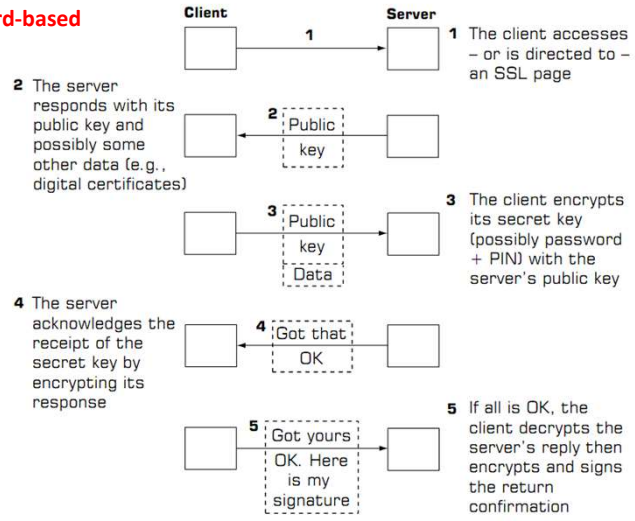
O : One
T : Time
P : Password



The security in this system is due to the fact that the password is never sent "across the wire"

Secure Sockets Layer (SSL)

password-based



Q & A