Bedeckt schreiben, leicht bekleidete Personen und Omas Geburtstag

Liebe Studenten Studierende!

Im heutigen Seminar werde ich lehren, wie man verbirgt, dass man etwas verschlüsselt hat. Die Methode nennt man <u>Steganografie</u>: Steganografie ist die Wissenschaft, Informationen in einem Trägermedium verborgen zu speichern und zu übermitteln. Das Wort lässt sich auf die griechischen Bestandteile στεγανός steganós ,bedeckt' und γράφειν gráphein ,schreiben' zurückführen, bedeutet also wörtlich "bedeckt schreiben" bzw. "geheimes Schreiben".

Man kann zum Beispiel einen Text in einer anderen Datei verbergen und dann verschicken. Ich zeige Euch gleich die Paranoia-Version: Wir verstecken einen verschlüsselten Text (den ohnehin nur der Empfänger wieder entschlüsseln kann), in einem Foto.

Man muss sich daran erinnern, dass es immer wieder ahnungslose Politiker gibt, die fordern, man müsse Verschlüsselung verbieten. Sollen Sie das doch tun! Wir würden mit Steganografie <u>glaubhaft abstreiten</u>, dass wir verschlüsselt haben.

Ich installiere zuerst das Programm <u>OpenStego</u>. Die freie Software gibt es für Windows und Linux. Ich führe Euch vor, wie das "geheime Schreiben" mit der Linux-Version geht.



2. Jetzt rufe ich <u>Kleopatra</u> auf und verschlüssele die Datei. In meinem Beispiel habe ich die Botschaft nur an mich selbst verschlüsselt. Der Text heißt jetzt message.txt.<u>gpg</u>.



Das Bild ist 450,5 Kilobyte groß. Das wird gleich noch einen Rolle spielen.

	OpenStego		×	
<u>F</u> ile <u>H</u> elp				
Data Hiding	Hide data in harmless looking f	iles		
Hide Data	Message File /home/burks/Downloads/message.txt.gpg Cover File			
Digital Watermarking (Beta)	/home/burks/Downloads/bildspaerlichbekleiderterpersonen.jpg			
Generate Signature	/home/burks/Downloads/omas_geburtstag.png			
Embed Watermark Verify Watermark	Options Encryption Algorithm Password	AES128		
	Confirm Password			
		Hide Dat	a	

Der bloße Augenschein, wenn man das Original und das jetzt erzeugte Bild vergleicht, sagt: die sind gleich?! Das Bild rechts ist das neue omas_geburtstag.png. [Beide Bilder sind nicht die Originale.]

Eigenschaften von omas_geburtstag.png							
Grund	legend Zugriffs	rechte	Öffnen mit	Bild			
	Name:	omas_geburt	stag.png				
3 27	Тур:	PNG-Bild (image/png)					
	Größe:	1,1 MB (1.124.9	986 Bytes)				
Übergeordneter Ordne		/home/burks/	Downloads				
	Zugegriffen: Geändert:	So 13 Dez 2020 So 13 Dez 2020	21:01:21 CET 21:01:11 CET				

5. Ich extrahiere jetzt die versteckte Datei aus dem Bild und wähle dafür den Menüpunkt *extract data*. Das Ergebnis will ich in meinem Ordner "Dokumente" speichern, damit die Original-Botschaft, die noch im Ordner "Downloads" liegt, nicht überschrieben wird.

	OpenStego	×
<u>F</u> ile <u>H</u> elp		
Data Hiding	Extract hidden data	
Hide Data	Input Stego File /home/burks/Downloads/omas_geburtstag.png Output Folder for Message File	
Digital Watermark Generate Sign Embed Watermark	Success Successfully extracted from the Cover file: message.txt.gpg	Extract Data
Verify Watermark		

Es hat funktioniert! Die Datei message.txt in meinem Ordner "Dokumente" kann ich jetzt wieder mit einem Editor lesen.

Als Hausaufgabe bitte ich euch, das Obige mit der Windows-Version von OpenStego zu exerzieren.