Some Privacy Solutions

- The Scott McNealy solution
  - "Get over it."
- Data encryption
- Anonymizers
- Onion routing
- Privacy-preserving data mining
- Preserving location privacy

Data Encryption for Privacy

- Store private data in encrypted form
- If the encrypted version is divulged, attacker might not be able to use it
  - Assuming strong crypto
  - And careful key management
- Particularly important for data on devices that are easily stolen
  - Portable computers, smart phones, flash drives

A Fundamental Issue

- Entities usually keep sensitive data because they want to process it
- They can't process encrypted data
- So they can usually decrypt it
- If the attacker can get the decrypted version, you lose
- Limits the benefit of crypto for privacy

Full Disk Encryption

- A useful solution for data on portable computers
  - Some laws regard such encrypted data as “safe”
- But only if key not available to a thief
  - So where did you get that key?

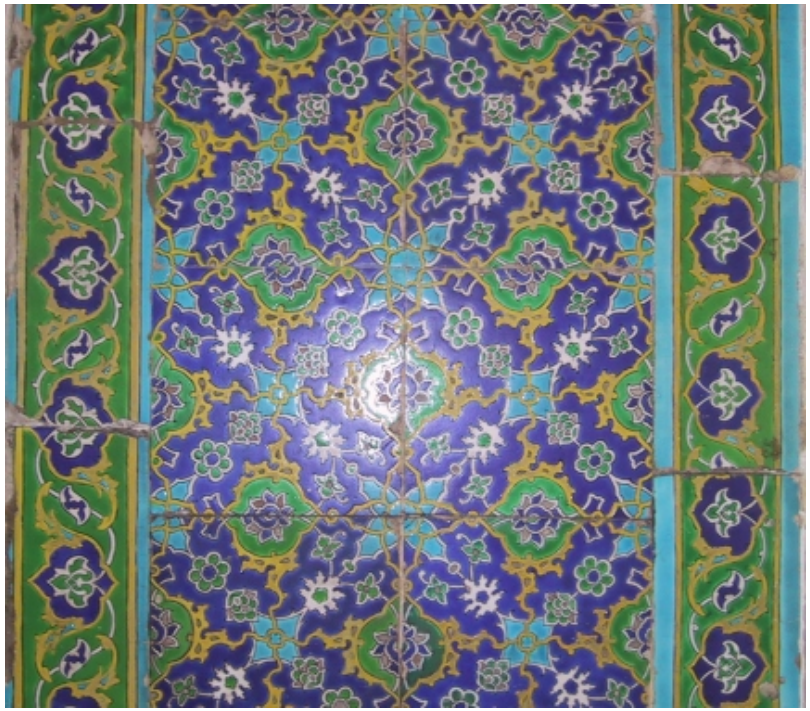
Homomorphic Cryptography

- An emerging research branch of cryptography
- Allows processing of encrypted data
  - Without ever decrypting it
- Successfully demonstrated, with important restrictions
- Generally too performance-expensive for practical use, so far

Steganography

- Another means of hiding data in plain sight
- In general terms, refers to embedding data into some other data
- In modern use, usually hiding data in an image
  - People have talked about using sound and other kinds of data

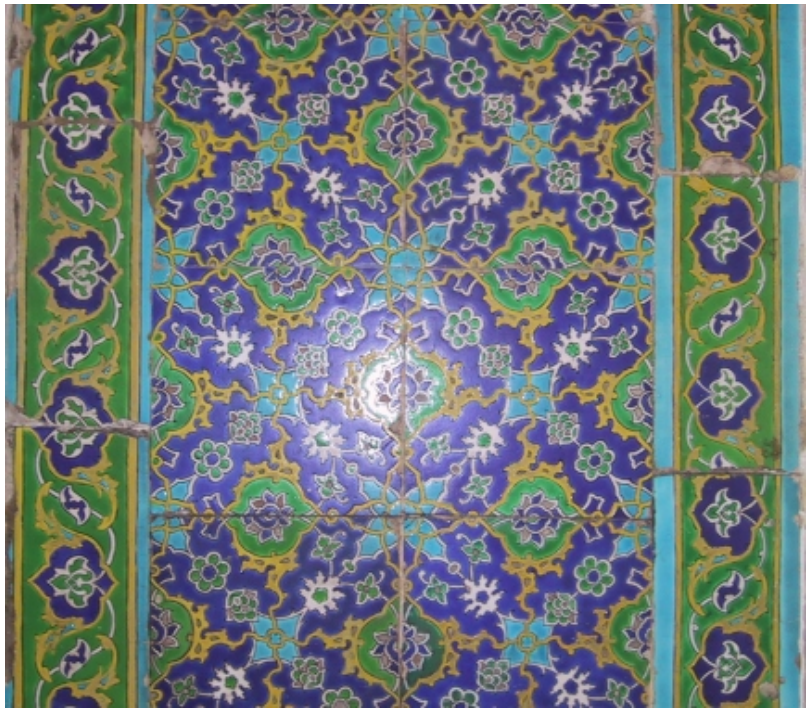
An Example

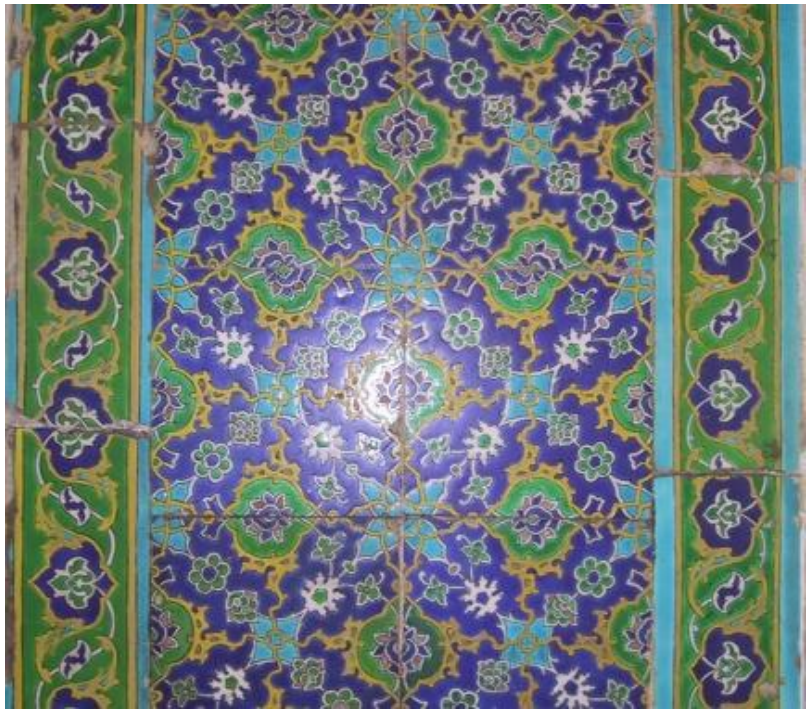


```
Transfer
$100 to my
savings
account
```

Run these through `outguess`

Voila!





The one on the right has the message hidden in it

How It Works

- Encode the message in the low order bits of the image
- Differences in these bits aren't human-visible
- More sophisticated methods also work
- Detected by looking for unlikely patterns
- Often foiled by altering images
- Steganography designers try to be robust against these problems

What's Steganography Good For?

- Used by some printer manufacturers to prove stuff came from them
- Stories of use by Al-Qaeda
  - No evidence of truth of stories
- Recent Shady Rat attacks apparently used it to hide code to contact botnet servers
- Russian spies used it recently
- Most useful if opponents don't suspect you're using it

Steganography and Privacy

- If they don't know my personal data is in my family photos, maybe it's safe
- But are you sure they don't know?
  - Analysis of data used to store things steganographically may show that
- Essentially, kind of like crypto
  - But without the same level of mathematical understanding

Anonymizers

- Network sites that accept requests of various kinds from outsiders
- Then submit those requests
  - Under their own or fake identity
- Responses returned to the original requestor
- A NAT box is a poor man's anonymizer

The Problem With Anonymizers

- The entity running it knows who's who
- Either can use that information himself
- Or can be fooled/compelled/hacked to divulge it to others
- Generally not a reliable source of real anonymity

An Early Example

- A remailer service in Finland
- Concealed the actual email address of the sender
  - By receiving the mail and resending it under its own address
- Court order required owner of service to provide a real address
  - After which he shut down the service