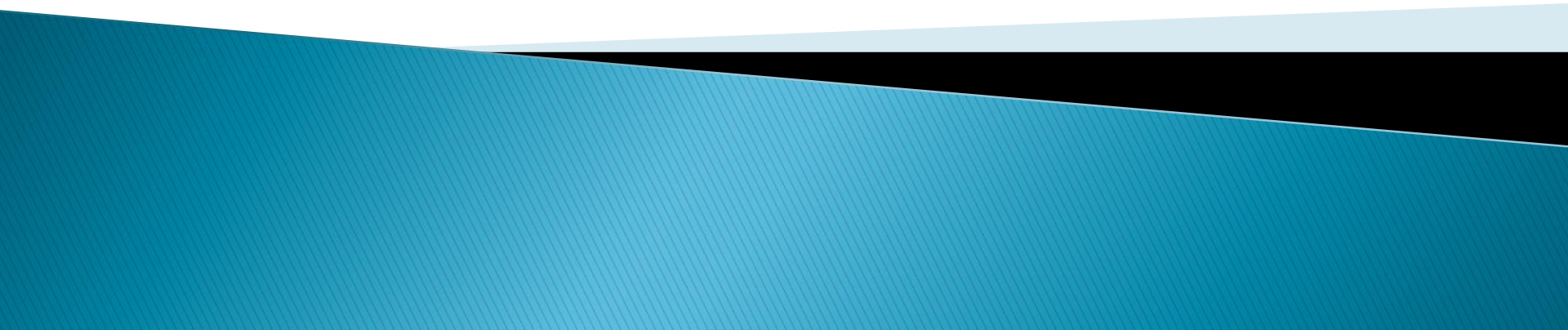
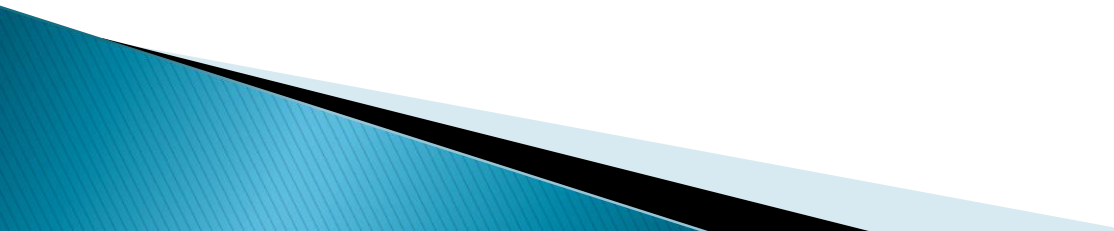


Introduction to Cryptology



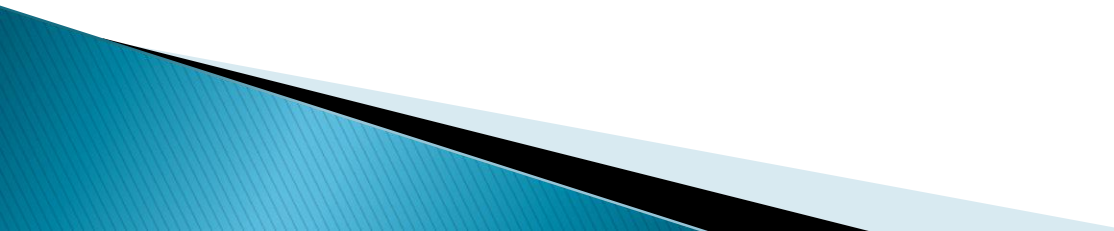
What is Cryptology?

- ▶ **Cryptography:** the science that studies the mathematical techniques for keeping messages secure.
 - ▶ **Cryptanalysis:** the science of defeating cryptography
 - ▶ **Cryptology:** the area of mathematics that studies cryptography and cryptanalysis.
- 

Why study cryptology ?

December 2, 2009: **Security Alert**

Microsoft and several security firms are warning users about protecting their account credentials during the holiday shopping season in the wake of an increasing number of people shopping for gifts online.



January 28, 2009: **The Heartland Case**

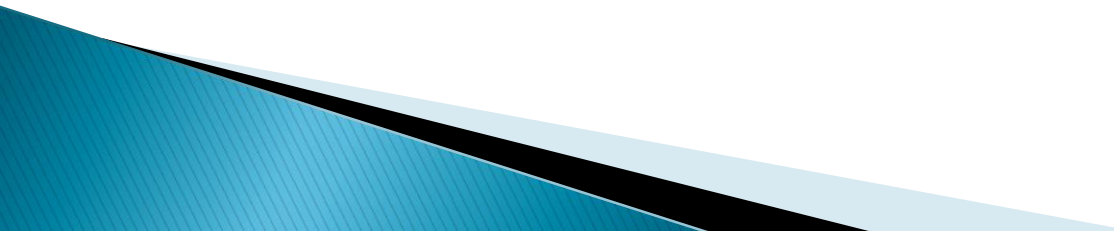
Who is Heartland?

A New Jersey company that processes credit cards for more than 250,000 businesses including retailers, restaurants, gas stations and grocery stores.

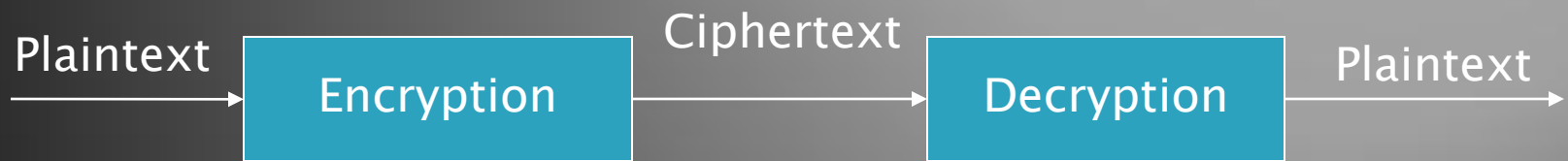
What was done?

Cyber criminals in 2008 planted a malicious software in Heartland's computer system and captured data from an untold number of transactions.

The Heartland Case

- ▶ Some analysts are describing this as the largest credit card security breach ever.
 - ▶ The captured information included names, card numbers, expiration dates and some internal bank codes contained within the cards.
- 

BASIC CONCEPTS



BASIC CONCEPTS

Key: Some critical information used for encryption (decryption)

Note:

1. Only two people with identical keys can encrypt and decrypt messages.
2. Someone with one key cannot decrypt messages encrypted with a different key.

Tools for achieving the goals of information security

- ▶ Key-agreement protocol,
- ▶ Cryptosystem,
- ▶ Digital Signatures,
- ▶ Certificates,
- ▶ Secure hardware,, and

Beautiful mathematics



Cryptosystem

Algorithm for key generation

+

Algorithm for encryption

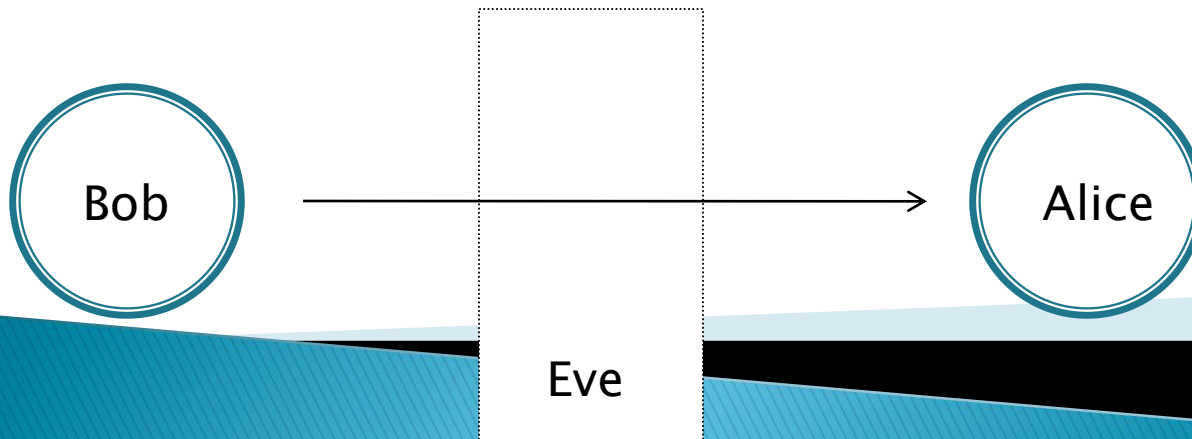
+

Algorithm for decryption

Cryptosystems

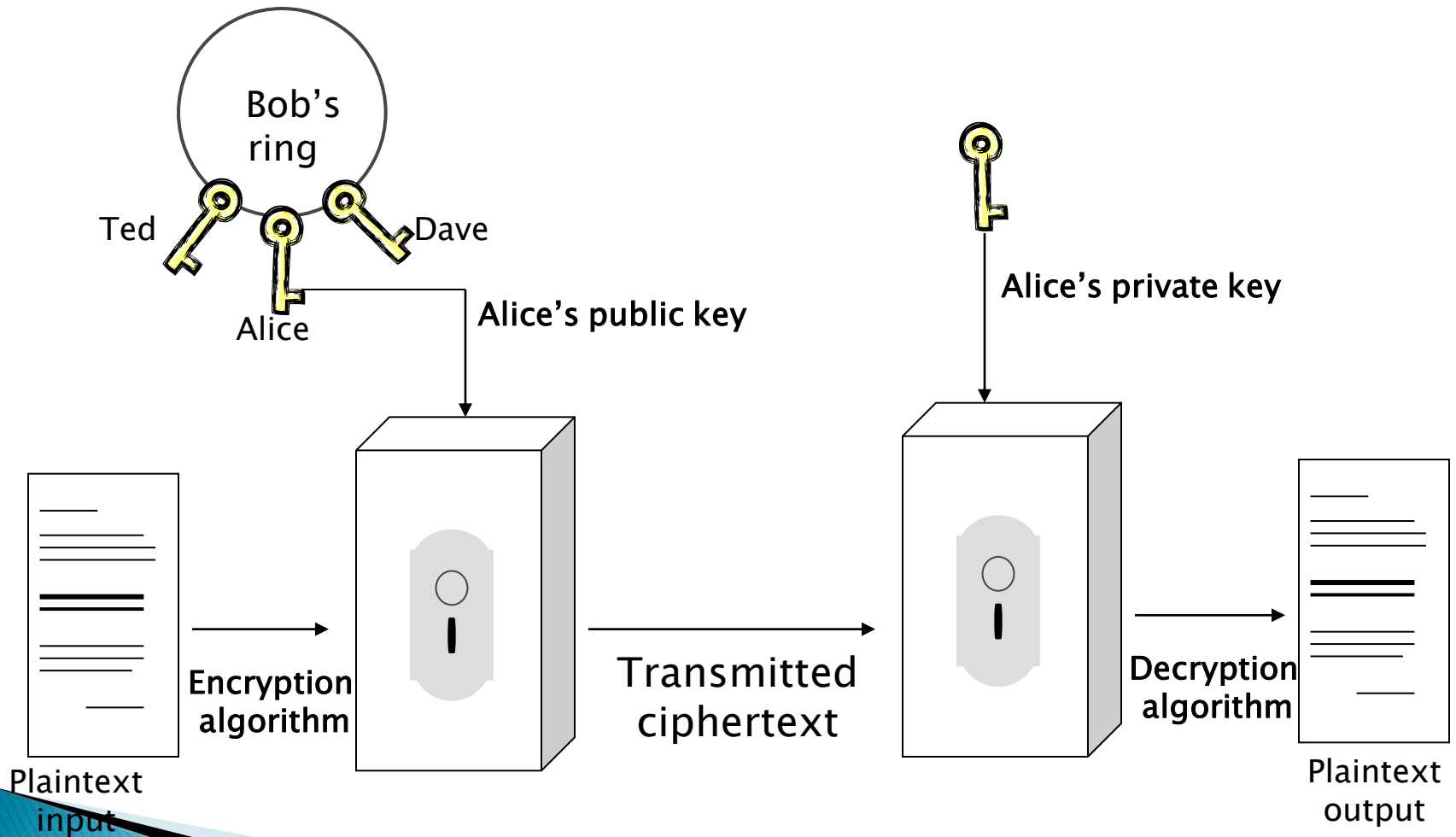
Terminology:

Sender and Receiver (Bob and Alice)



Eve – eavesdropper

Public-key cryptosystem



RSA cryptosystem

Key Generation Algorithm

1. Choose two primes p and q
2. Compute $n=pq$
3. Compute $\phi(n)=(p-1)(q-1)$
4. Choose a random number x such that $\gcd(x,\phi(n))=1$
5. Compute $e=1/x \bmod \phi(n)$

Public key: n, e

Private key: x

RSA cryptosystem

Encryption Algorithm

1. Convert a message into a number M
2. Compute $E = M^e \pmod n$

Ciphertext: E



RSA cryptosystem

Decryption Algorithm

1. Compute $D = E^x \bmod n$

The decryption algorithm works:

$$D = M$$

Fermat factoring method

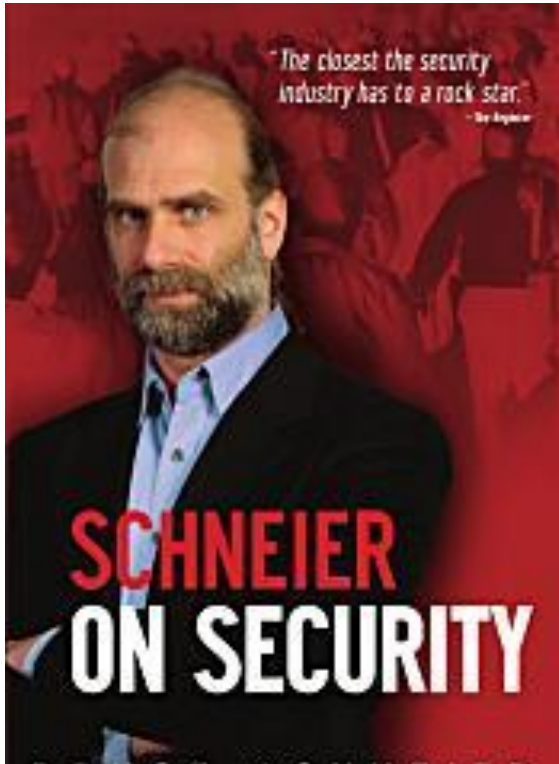
Theorem

Any odd integer is a difference of two squares.

Corollary

If $n=pq$ then $n= [(p + q) / 2]^2 - [(p - q) / 2]^2$

February 4, 2010 at BSU



“The computer systems we use on our desktops are not reliable enough for critical applications.

Neither is the Internet.

The more we rely on them in our critical infrastructure, the more vulnerable we become.

The more our systems become interconnected, the more vulnerable we become.”

Bruce Schneier

Chief Security Technology Officer of BT