Instructor: Gene Tsudik
Email: gts@ics.uci.edu
Phone: (949) 824-3410
Office: ICS 458

- Lectures: 9:30-10:50 Mo/We
- Office Hours (tentative):
  - 10:00-11:00 Tu
  - 9:30-10:30 Fr
- TA: none , Graders: none
- Grading: 2 hws (20% ea), midterm (30%), project (30%) - tentative!
- Web page: www.ics.uci.edu/~gts/268
- Mailing list: 36592-f01@classes.uci.edu

Your Project:

- Theory: new result or paper survey with some insight
- Hacking: firewalls, linux security
- Experiments: performance of (e.g.) SSL/TLS
- Etc., etc...

Write 1-page Proposal, due by October 15.

Textbooks:

- REQUIRED: Douglas R. Stinson, *Cryptography (Theory and Practice)*, CRC Press, ISBN 0-8493-8521-0
- SUPPLEMENTAL: William Stallings, *Cryptography and Network Security (second edition), PRENTICE-HALL, ISBN 0-13-869017-0*

Rules and Guidelines

- Lecture notes
- Homework policy
- Using the web and other reference material
- Collaboration
- Using course mailing list
- Problems, issues, suggestions, etc.
- Course Evaluation
- Dropping the course: 3 WEEKS
- Resources
- Difficulty level
- Other topics?

Topic Outline (tentative):

1. Introduction: History, Terminology, Threats and Attacks, Information Theory + Probability
2. Block ciphers, DES: history, design, modes of operation, Number Theory concepts
3. Public Key Cryptography: Merkle, Diffie-Hellman, RSA, Rabin, El Gamal, Knapsack
4. PK Digital Signatures: RSA, DSA, Cryptographic Hash functions: MD5, SHA
5. One-Times Signatures, Key Management: Establishment/Distribution/Agreement
6. Trusted Third Parties: Kerberos, etc., Certification and Revocation: CAs, CRLs, etc.
7. Identification/Authentication schemes: Schnorr, Okamoto, Guillou-Quisquater, Secret Sharing and PRNGs
8. Program Security: Viruses, worms, trojan horses, etc. Countermeasures and counterattacks.
9. Internet Cryptography: IPSEC, ISA-KMP, DNSSEC; Other "stansards": PGP, SSL, SET
10. Advanced Topics and Review

Basic Terminology

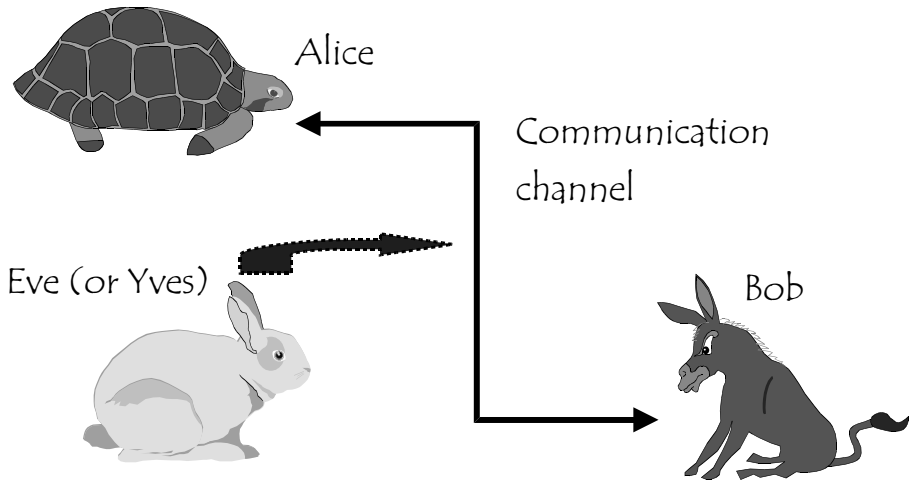
Cryptography

- Cryptology, Cryptography, Cryptanalysis
- Cipher, Cryptosystem
- Encryption/Decryption, Encipher/Decipher
- Privacy, Authentication & Identification
- Integrity
- Non-repudiation
- Freshness, Timeliness, Causality
- Intruder, Adversary, Interloper, etc.
- Anonymity, Unlinkability

Computer security

- Access Control & Authorization
- Accountability
- Intrusion Detection
- Physical Security
- Tamper-resistance
- Certification & Revocation
- Availability

The cast of characters

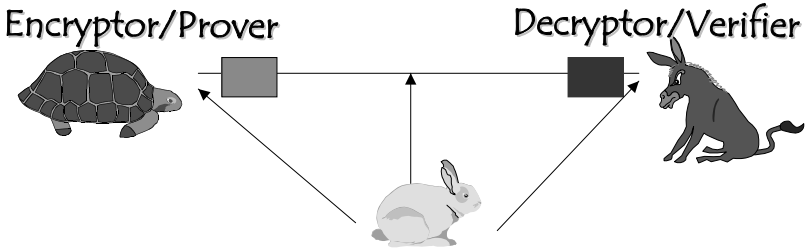


Crypto Attacks:

- ciphertext only
- known plaintext
- chosen plaintext
- chosen ciphertext
- brute force

Cryptosystem:

- *P -- plaintext*
- *C -- ciphertext*
- *K -- keyspace*
- *E -- encryption rules*
- *D -- decryption rules*



Complexity Theory

P: problems that can be solved in polynomial time, i.e., problems that can be solved "efficiently"

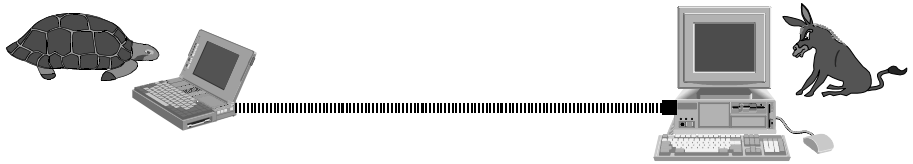
NP: broad set of problems that includes P

NP-complete: the hardest problems in NP, they appear to have no efficient solution

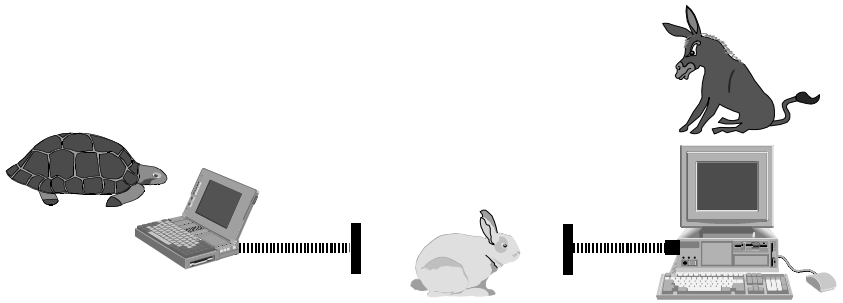
Factoring, discrete log are in NP, not known to be NP-complete or in P

Security Attacks

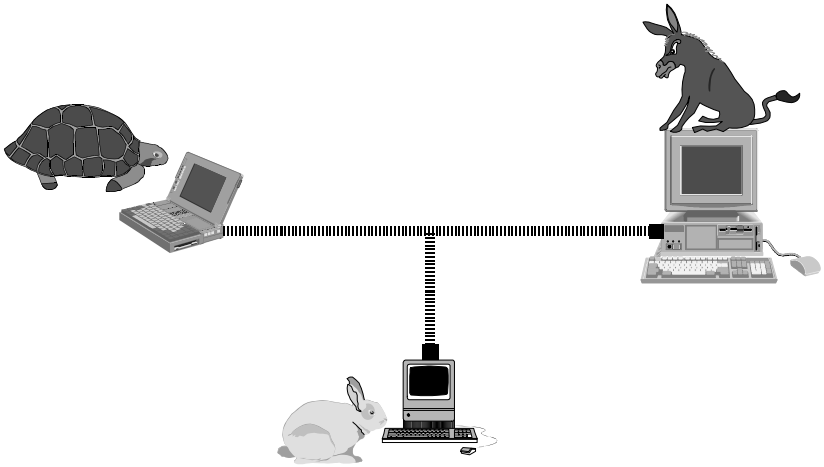
- Passive Attacks, e.g., eavesdropping
- Active Attacks, e.g., interruption



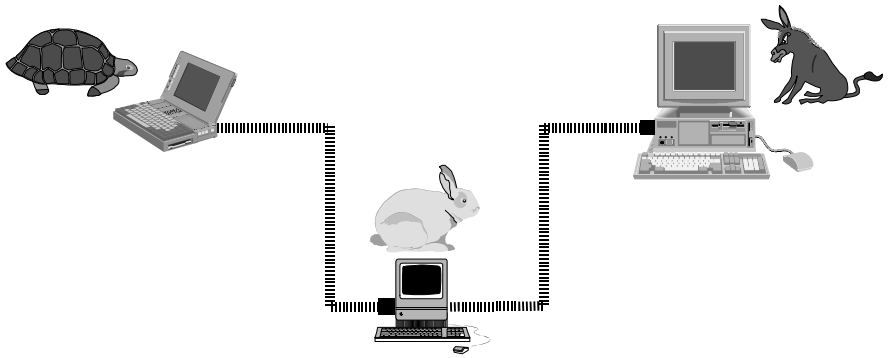
Security Attacks (1)
Interruption



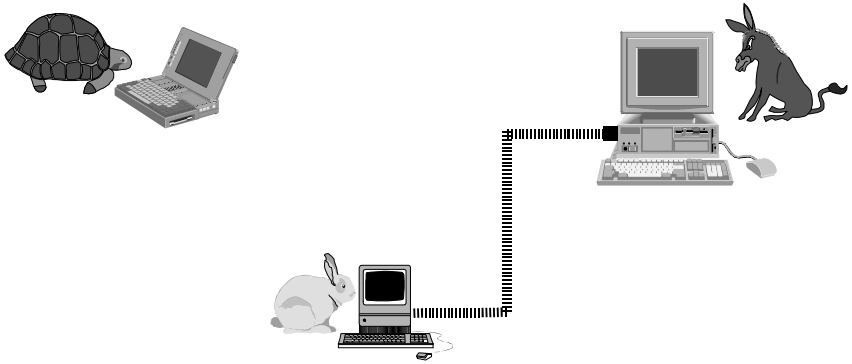
Security Attacks (2)
Interception



Security Attacks (3)
Modification



Security Attacks (4)
Injection



Security Mechanisms

- Cryptography
- Firewalls
- Security protocols, IP/virus protection, etc.
- Hardware Protection
- Ad-hoc Techniques
- .....

Some preliminary math

- Exclusive-OR, XOR
- Primality, relative
- Groups, Rings, Fields
- Modular Arithmetic
- Probability (later)

Some preliminary math

Properties of operators:

- Closure
- Commutativity (a+b)=(b+a)
- Associativity (a+b)+c=a+(b+c)
- Identity (a+I)=a
- Inverse
- Mult-n distributes over addition

Some preliminary math

Multiplicative Inverse:

$$a^{-1} \ni a * a^{-1} = 1$$

Additive Inverse:

$$a^{-1} \ni a + a^{-1} = 0$$

Example:

$$Z_{11} = \{0,1,2,3,4,5,6,7,8,9,10\}$$
$$+\,inverses = \{-,10,9,8,7,6,5,4,3,2,1\}$$
$$*\,inverses = \{-,1,6,4,3,9,2,8,7,5,10\}$$

Does multilicative inverse alwas exist? e.g., 3^{-1} in Z_{12}

Simple Ciphers

- Shift Cipher (e.g., Caesar's shift by 3)
- Substitution Cipher (Bible)
- The most secure cipher: ONE-TIME PAD

$$\text{Plaintext} = \{p_0,\ldots,p_{n-1}\}$$
$$\text{One - time pad stream} = \{otp_0,\ldots,otp_{n-1}\}$$
$$\text{Ciphertext} = \{c_0,\ldots,c_{n-1}\}$$

where:

$$c_i = p_i \oplus otp_i \forall 0 < i < n$$

The Shift Cipher

Definition:

$a \equiv b \bmod n$ if and only if $a \bmod n = b \bmod n$

$$a = q_1 n + r_1 \qquad r_1 = a \bmod n$$
$$b = q_2 n + r_2 \qquad r_2 = b \bmod n$$

$$0 \leqslant r_1, r_2 \leqslant n-1$$

The Shift Cipher (1)

Definition: $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

Example:

$11 \cdot 13 \bmod 16 \in \mathbb{Z}_{16}$

$11 \cdot 13 = 143 \Rightarrow 143 \bmod 16 \Rightarrow 143 = 8 \cdot 16 + 15$

$11 \cdot 13 \bmod 16 = 15$

The Shift Cipher (2)

$A = 0, B = 1, C = 2, D = 3, \ldots\ldots, Z = 25$

$P, C, K \in \mathbb{Z}_{26}$

$$e_K(p) = p + K \bmod 26$$

$$d_K(c) = c - K \bmod 26$$

The Shift Cipher (3)

Example:

$K = 11$

W	*E*	*W*	*I*	*L*	*L*	*M*	*E*	*E*	*T*	*A*	*T*	*M*	*I*	*D*	*N*	*I*	*G*	*H*	*T*
22	4	22	8	11	11	12	4	4	19	0	19	12	8	3	13	8	6	7	19
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
7	15	7	19	22	22	23	15	15	4	11	4	23	19	14	24	19	17	18	4
H	*P*	*H*	*T*	*W*	*W*	*X*	*P*	*P*	*E*	*L*	*E*	*X*	*T*	*O*	*Y*	*T*	*R*	*S*	*E*

The Shift Cipher (4)

Cryptanalysis

H	P	H	T	W	W	X	P	P	E	L	E	X	T	O	Y	T	R	S	E
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
7	15	7	19	22	22	23	15	15	4	11	4	23	19	14	24	19	17	18	4

$$(mean\ no.\ of\ trials)\ T = \frac{26}{2} = 13$$

See also page 6 in book

The Substitution Cipher

Example:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
X	N	Y	A	H	P	O	G	Z	Q	W	B	T	S	F	L	R	C	V	M	U	E	K	J	D	I

$$\pi(D) = A, \pi(P) = L, \pi(Z) = I, \ldots$$

W	E	W	I	L	L	M	E	E	T	A	T	M	I	D	N	I	G	H	T
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
K	H	K	Z	B	B	T	H	H	M	X	M	T	Z	A	S	Z	O	G	M

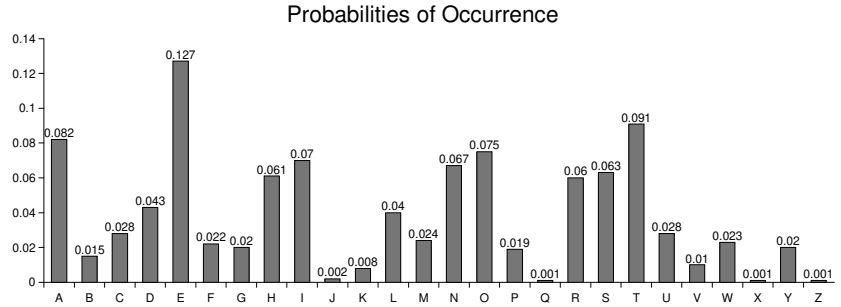
The Substitution Cipher (1)

$x, y \in \mathbb{Z}_{26}$

$$e_\pi(x) = \pi(x)$$
$$d_\pi(y) = \pi^{-1}(y)$$

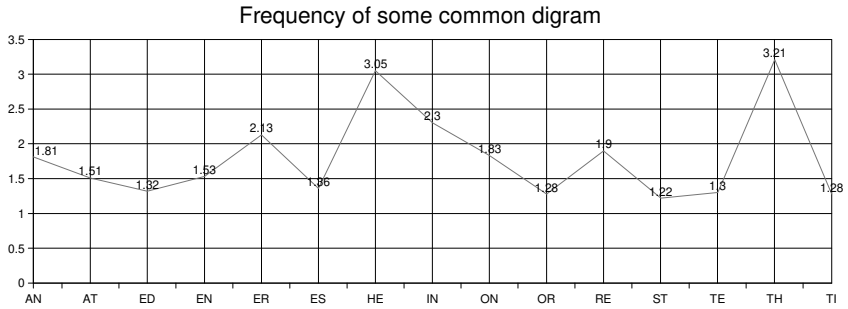
The Substitution Cipher (2)

Cryptanalysis $26! > 4.0 \times 10^{26}\ keys$



The Substitution Cipher (3)

Cryptanalysis



For next time...

- Read Chapter 1 in Stinson's book
- Think about projects