CSE 484: Computer Security and Privacy

Cryptography
[Symmetric Encryption]

Spring 2021

Tadayoshi Kohno
yoshi@cs

Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, David Kohlbrenner, Yoshi Kohno, Ada Lerner, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...
History: Substitution Cipher

- **Superset of shift ciphers**: each letter is substituted for another one.
- One way to implement: **Add a secret key**
- Example:
  - Plaintext: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
  - Cipher: `ZEBRASCDFGHIJKLMNOPQRSTUVWXYZ`
- "State of the art" for thousands of years
History: Substitution Cipher

- What is the key space?
- How to attack?
  - Frequency analysis.

26! \approx 2^{88}

**Bigrams:**

<table>
<thead>
<tr>
<th>1st Character</th>
<th>2nd Character</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>th</td>
<td>en</td>
<td>1.52%</td>
</tr>
<tr>
<td>he</td>
<td>ed</td>
<td>1.28%</td>
</tr>
<tr>
<td>in</td>
<td>to</td>
<td>0.94%</td>
</tr>
<tr>
<td>er</td>
<td>it</td>
<td>0.94%</td>
</tr>
<tr>
<td>an</td>
<td>ou</td>
<td>0.82%</td>
</tr>
<tr>
<td>re</td>
<td>ea</td>
<td>0.68%</td>
</tr>
<tr>
<td>nd</td>
<td>hi</td>
<td>0.63%</td>
</tr>
<tr>
<td>at</td>
<td>is</td>
<td>0.59%</td>
</tr>
<tr>
<td>on</td>
<td>or</td>
<td>0.57%</td>
</tr>
<tr>
<td>nt</td>
<td>ti</td>
<td>0.56%</td>
</tr>
<tr>
<td>ha</td>
<td>as</td>
<td>0.56%</td>
</tr>
<tr>
<td>es</td>
<td>te</td>
<td>0.56%</td>
</tr>
<tr>
<td>st</td>
<td>et</td>
<td>0.55%</td>
</tr>
<tr>
<td>en</td>
<td>ng</td>
<td>0.55%</td>
</tr>
<tr>
<td>ed</td>
<td>of</td>
<td>0.53%</td>
</tr>
<tr>
<td>to</td>
<td>al</td>
<td>0.52%</td>
</tr>
<tr>
<td>it</td>
<td>de</td>
<td>0.50%</td>
</tr>
<tr>
<td>ou</td>
<td>se</td>
<td>0.50%</td>
</tr>
<tr>
<td>ea</td>
<td>le</td>
<td>0.47%</td>
</tr>
<tr>
<td>hi</td>
<td>sa</td>
<td>0.46%</td>
</tr>
<tr>
<td>is</td>
<td>si</td>
<td>0.46%</td>
</tr>
<tr>
<td>or</td>
<td>ar</td>
<td>0.43%</td>
</tr>
<tr>
<td>ti</td>
<td>ve</td>
<td>0.34%</td>
</tr>
<tr>
<td>as</td>
<td>ra</td>
<td>0.33%</td>
</tr>
<tr>
<td>te</td>
<td>ld</td>
<td>0.27%</td>
</tr>
<tr>
<td>et</td>
<td>ur</td>
<td>0.19%</td>
</tr>
<tr>
<td>ng</td>
<td>of</td>
<td>0.18%</td>
</tr>
<tr>
<td>al</td>
<td>de</td>
<td>0.16%</td>
</tr>
<tr>
<td>le</td>
<td>sa</td>
<td>0.06%</td>
</tr>
<tr>
<td>si</td>
<td>ar</td>
<td>0.05%</td>
</tr>
<tr>
<td>sa</td>
<td>ra</td>
<td>0.04%</td>
</tr>
<tr>
<td>ra</td>
<td>ld</td>
<td>0.02%</td>
</tr>
<tr>
<td>ur</td>
<td>te</td>
<td>0.02%</td>
</tr>
</tbody>
</table>

**Trigrams:**

1. the 6. ion 11. nce  
2. and 7. tio 12. edt  
3. tha 8. for 13. tis  
4. ent 9. nde 14. oft  
5. ing 10. has 15. sth
History: Enigma Machine

Uses rotors (substitution cipher) that change position after each key.

Key = initial setting of rotors

Key space?

$26^n$ for $n$ rotors
How Cryptosystems Work Today

• **Layered approach:** Cryptographic protocols (like “CBC mode encryption”) built on top of cryptographic primitives (like “block ciphers”)
• **Flavors of cryptography:** Symmetric (private key) and asymmetric (public key)
• Public algorithms (**Kerckhoff’s Principle**)
• Security proofs based on assumptions (**not this course**)

• Be careful about inventing your own! (If you just want to use some crypto in your system, use vetted libraries!)
The Cryptosystem Stack

• Primitives:
  • AES / DES / etc
  • RSA / ElGamal / Elliptic Curve (ed25519)

• Modes:
  • Block modes (CBC, ECB, CTR, GCM, ...)
  • Padding structures

• Protocols:
  • TLS / SSL / SSH / etc

• Usage of Protocols:
  • Browser security
  • Secure remote logins
Kerckhoff’s Principle

• Security of a cryptographic object **should depend only on the secrecy of the secret (private) key.**

• Security should not depend on the secrecy of the algorithm itself.

• Foreshadow: Need for randomness – the key to keep private
Flavors of Cryptography

• Symmetric cryptography
  • Both communicating parties have access to a shared random string $K$, called the key.

• Asymmetric cryptography
  • Each party creates a public key $pk$ and a secret key $sk$.
  • Hard concept to understand, and revolutionary! Inventors won Turing Award 😊
Symmetric Setting

Both communicating parties have access to a shared random string $K$, called the key.
Asymmetric Setting

Each party creates a public key $pk$ and a secret key $sk$. 

Alice

- $pk_A, sk_A$
- $pk_B, sk_A$

Bob

- $pk_A, sk_B$
- $pk_B, sk_B$

Adversary

- $pk_A, sk_B$
- $pk_B, sk_A$
A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.

2. A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems.
Flavors of Cryptography

• Symmetric cryptography
  • Both communicating parties have access to a shared random string $K$, called the key.

• Asymmetric cryptography
  • Each party creates a public key $pk$ and a secret key $sk$. 
Flavors of Cryptography

• Symmetric cryptography
  • Both communicating parties have access to a shared random string $K$, called the key.
  • Challenge: How do you privately share a key?

• Asymmetric cryptography
  • Each party creates a public key $pk$ and a secret key $sk$.
  • Challenge: How do you validate a public key?
Flavors of Cryptography

• Symmetric cryptography
  • Both communicating parties have access to a *shared random string* $K$, called the key.
  • Challenge: How do you privately share a key?

• Asymmetric cryptography
  • Each party creates a public key $pk$ and a secret key $sk$.
  • Challenge: How do you validate a public key?

• Key building block: Randomness – something that the adversaries won’t know and can’t predict and can’t figure out
Ingredient: Randomness

• Many applications (especially security ones) require randomness
• Explicit uses:
  • Generate secret cryptographic keys
  • Generate random initialization vectors for encryption
• Other “non-obvious” uses:
  • Generate passwords for new users
  • Shuffle the order of votes (in an electronic voting machine)
  • Shuffle cards (for an online gambling site)
C’s rand() Function

• C has a built-in random function: `rand()`

```c
unsigned long int next = 1;
/* rand: return pseudo-random integer on 0..32767 */
int rand(void) {
    next = next * 1103515245 + 12345;
    return (unsigned int)(next/65536) % 32768;
}
/* srand: set seed for rand() */
void srand(unsigned int seed) {
    next = seed;
}
```

• Problem: don’t use `rand()` for security-critical applications!
  • Given a few sample outputs, you can predict subsequent ones
mamajoe: Hey guys, Big B is in!
More details: “How We Learned to Cheat at Online Poker: A Study in Software Security”
PS3 and Randomness

Hackers obtain PS3 private cryptography key due to epic programming fail? (update)


- 2010/2011: Hackers found/released private root key for Sony’s PS3
- Key used to sign software – now can load any software on PS3 and it will execute as “trusted”
- Due to bad random number: same “random” value used to sign all system updates