Recap

1. Shift Cipher: Crackable. Keyspace has only 26 elements.
2. Affine Cipher: Crackable. Keyspace has only 312 elements.
3. Vig Cipher: Crackable by repeats and letter freqs.
5. Matrix Cipher: Crackable if know (Enc,Dec)-pairs.
6. RSA: Uncrackable if we make hardness assumptions.
7. One-Time Pad: Uncrackable!
Recap

1. Shift Cipher: Crackable. Keyspace has only 26 elements.
2. Affine Cipher: Crackable. Keyspace has only 312 elements.
3. Vig Cipher: Crackable by repeats and letter freqs.
5. Matrix Cipher: Crackable if know (Enc,Dec)-pairs.
6. RSA: Uncrackable if we make hardness assumptions.
7. One-Time Pad: Uncrackable!

All of the above are true.
Recap

1. Shift Cipher: Crackable. Keyspace has only 26 elements.
2. Affine Cipher: Crackable. Keyspace has only 312 elements.
3. Vig Cipher: Crackable by repeats and letter freqs.
5. Matrix Cipher: Crackable if know (Enc, Dec)-pairs.
6. RSA: Uncrackable if we make hardness assumptions.
7. One-Time Pad: Uncrackable!

All of the above are true.
All of the above are not rigorous!
Recap

1. Shift Cipher: Crackable. Keyspace has only 26 elements.
2. Affine Cipher: Crackable. Keyspace has only 312 elements.
3. Vig Cipher: Crackable by repeats and letter freqs.
5. Matrix Cipher: Crackable if know (Enc,Dec)-pairs.
6. RSA: Uncrackable if we make hardness assumptions.
7. One-Time Pad: Uncrackable!

All of the above are true.
All of the above are not rigorous!
We make them ... more rigorous
Assumptions

- With few exceptions, cryptography currently requires *computational assumptions*
  
  - Question: If $P \neq NP$ was proven then would we still need to make hardness assumptions? Discuss with your neighbor.
Assumptions

- With few exceptions, cryptography currently requires *computational assumptions*
  
  - Question: If $P \neq NP$ was proven then would we still need to make hardness assumptions? Discuss with your neighbor.

$P \neq NP$ not good enough!

Factoring and Discrete Log are not $NP$-complete and are thought to *not* be $NP$-complete. Possible that:

1. $SAT \not\in P$
2. Factoring is in $P$. 

Assumptions

- With few exceptions, cryptography currently requires *computational assumptions*

  - Question: If $P \neq NP$ was proven then would we still need to make hardness assumptions? Discuss with your neighbor.

    $P \neq NP$ not good enough!
    Factoring and Discrete Log are not $NP$-complete and are thought to not be $NP$-complete. Possible that:
    1. $SAT \notin P$
    2. Factoring is in $P$.

- Principle: Need assumptions to be explicit
Importance of clear assumptions

- Allow researchers to (attempt to) validate assumptions by studying them

- Allow meaningful *comparison* between schemes based on different assumptions

- Useful to understand minimal assumptions needed

- Practical implications if assumptions are wrong

- Enable proofs of security
Proofs of Security/Limitations

Proofs give an iron-clad guarantee of security relative to the definition and assumptions! Provably secure schemes can be broken!

1. If the definition does not correspond to the real-world threat model
2. i.e. if attacker can go “outside the security mode”
3. If the assumption is invalid
4. If the implementation is flawed

All four of these happen in the real world.
Examples

1. Outside the Box: I’m from IT and I’m here to help.
2. Outside the Box: Timing attacks. To quote Wikipedia:

   A *timing attack is a side channel attack where in which the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms

   **Example:** In RSA the amount of time it takes to decrypt gives a rough idea of the size of the primes involved, cutting down search space.

3. Bad Implementations of Diffie-Helman
   3.1 Pick \( p \) two small.
   3.2 Pick \( g \) too small.
   3.3 Pick \( a, b \) too small. (But \( a, b \) random. How to fix?)
   3.4 Use same \( p, g \) for a year. Eve has a year to build DL tables.

4. Look up the story of the Maginot Line, an immense wall that France build to deter a German Invasion. It didn’t work.
Nevertheless... 

- This does not detract from the importance of having formal definitions in place
- This does not detract from the importance of proofs of security
Defining secure encryption
Crypto definitions (generally)

▶ Security guarantee/goal
  ▶ What we want to achieve and/or what we want to prevent the attacker from achieving

▶ Threat model
  ▶ What (real-world) capabilities the attacker is assumed to have
Threat models for encryption

- **Ciphertext-only attack (CTA).** As name indicates, Eve only has access to the ciphertext. Eve can crack Shift, Affine, Vig, Gen. Matrix might be an open problem if text is long enough.

- **Known-plaintext attack (KPA).** Eve has access to previous plaintexts and what the ciphertext was. Matrix can be cracked this way if text is long enough.

- **Chosen-plaintext attack (CPA).** Eve can fool Alice into encoding a particular plaintext.

- **Chosen ciphertext attack (CCA).** Eve can fool Bob into telling her what a particular ciphertext decodes to.
Goal of secure encryption?

- How would you define what it means for encryption scheme \((\text{Gen, Enc, Dec})\) over message space \(\mathcal{M}\) to be secure?
  - Against a (single) ciphertext-only attack
Secure encryption?

- “Impossible for the attacker to learn the key”
  - The key is a *means to an end*, not the end itself
  - Necessary (to some extent) but not sufficient
  - Easy to design an encryption scheme that hides the key completely, but is insecure
  - Can design schemes where most of the key is leaked, but the scheme is still secure
Secure encryption?

▶ “Impossible for the attacker to learn the plaintext from the ciphertext”

▶ What if the attacker learns 90% of the plaintext?
Secure encryption?

- “Impossible for the attacker to learn any character of the plaintext from the ciphertext”
  - What if the attacker is able to learn (other) partial information about the plaintext?
    - e.g. salary is greater than $75K
  - What if the attacker guesses a character correctly?
Perfect Secrecy
Perfect secrecy

- “Regardless of any prior information the attacker has about the plaintext, the ciphertext should leak no additional information about the plaintext”
  - The right notion!
  - How to formalize?
Probability review

- **Random variable (r.v.):** variable that takes on (discrete) values with certain probabilities

- Probability distribution for a r.v. specifies the probabilities with which the variable takes on each possible value
  - Each probability must be between 0 and 1
  - The probabilities must sum to 1
1. $k$ is a RV unif on $\{0, \ldots, 25\}$. Dist is $(\forall k)[\Pr(k) = \frac{1}{26}]$

2. CMSC/MATH 456 has 115 students, 85 in G’s class and 30 in R’s class. RV: $X$: Pick a student unif, and if G’s class then $X = 10$, if R’s class then $X = 20$.

\[
\Pr(X = 10) = \frac{85}{115} = \frac{17}{23}
\]
\[
\Pr(X = 20) = \frac{30}{115} = \frac{6}{23}.
\]
**Probability review**

- **Event**: a particular occurrence in some experiment
  - $\Pr[E]$: probability of event $E$

- Conditional probability: probability that one event occurs, *given that some other event occurred*
  - $\Pr[A|B] = \frac{\Pr[A \land B]}{\Pr[B]}$

- To RV's $X, Y$ are *independent* if for all $x, y$:
  - $\Pr[X = x|Y = y] = \Pr[X = x]$

  **Important**: Knowing that $Y = y$ does not help you figure out if $X = x$. 
Law of total probability say $E_1, \ldots, E_n$ are a partition of all possibilities. Then for any $A$:

$$
\Pr[A] = \sum_i \Pr[A \cap E_i] = \sum_i \Pr[A | E_i] \cdot \Pr[E_i]
$$
Probability distributions

Let $M$ be the random variable denoting the value of the message. $M$ ranges over $\mathcal{M}$.

Let's say $\mathcal{M}$ is the foll statements with the foll probs.

1. Today 456 went well. $Pr = \frac{1}{2}$.
2. Today 456 went badly. $Pr = \frac{1}{100}$.
3. All 456 students submitted HW Monday. $Pr = \frac{1}{100}$.
4. I proved a new result in crypto. $Pr = \frac{1}{50}$.
5. I proved a new result about The Muffin Problem. $Pr = \frac{9}{25}$.
6. I saw a student in office hours. $Pr = \frac{1}{10}$

Note:

1) This is the prob I send that msg, not that it happened.
2) Should we assume that Eve knows this distribution? Discuss with neighbor.
Recall

- A *private-key encryption scheme* is defined by a message space $\mathcal{M}$ and algorithms (Gen, Enc, Dec):
  - **Gen** (key generation algorithm) generates $k$
  - **Enc** (encryption algorithm): takes key $k$ and message $m \in \mathcal{M}$ as input; outputs ciphertext $c$
    \[
    c \leftarrow \text{Enc}_k(m)
    \]
  - **Dec** (decryption algorithm): takes key $k$ and ciphertext $c$ as input; outputs $m$
    \[
    m := \text{Dec}_k(c)
    \]
Notation

- $\mathcal{K}$ (key space) — set of all possible keys
- $\mathcal{M}$ (message space) — set of all possible messages
- $\mathcal{C}$ (ciphertext space) — set of all possible ciphertexts
Probability distributions

- Let $K$ be the random variable denoting the key
  - $K$ ranges over $\mathcal{K}$

- Fix some encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$
  - Gen defines a probability distribution for $K$:
    $$\Pr[K = k] = \Pr[\text{Gen outputs key } k]$$
    Usually Uniform.
Probability distributions

- Random variables M and K are *independent*
  - i.e., the message that a party sends does not depend on the key used to encrypt that message
Probability distributions

- Fix some encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) and some distribution for \(M\)

- Consider the following (randomized) experiment:
  1. Choose a message \(m\), according to the given distribution
  2. Generate a key \(k\) using \(\text{Gen}\)
  3. Compute \(c \leftarrow \text{Enc}_k(m)\)

- This defines a distribution on the ciphertext!

- Let \(C\) be a random variable denoting the value of the ciphertext in this experiment
Example 1

- Consider the shift cipher
  - So for all \( k \in \{0, \ldots, 25\} \), \( \Pr[K = k] = \frac{1}{26} \)

- Say \( \Pr[M = a] = 0.7 \), \( \Pr[M = z] = 0.3 \). So the message is ONLY 1 character.

- What is \( \Pr[C = b] \)?
  - Either \( M = a \) and \( K = 1 \), or \( M = z \) and \( K = 2 \)

\[
\Pr[C = b] = \Pr[M = a] \cdot \Pr[K = 1] + \Pr[M = z] \cdot \Pr[K = 2] \\
= 0.7 \cdot \frac{1}{26} + 0.3 \cdot \frac{1}{26} = \frac{1}{26}
\]

\( \frac{1}{26} \)? Hmmm? What if we had diff prob of messages. If replace 0.7 with \( p \) and 0.3 with \( 1 - p \) do we still get \( \frac{1}{26} \)? Discuss with neighbor without doing calculation.
Example 2

- Consider the shift cipher
  - So for all $k \in \{0, \ldots, 25\}$, $\Pr[K = k] = \frac{1}{26}$

- Say $\Pr[M = a] = p$, $\Pr[M = z] = 1 - p$. So the message is ONLY 1 character.

- What is $\Pr[C = b]$?
  - Either $M = a$ and $K = 1$, or $M = z$ and $K = 2$

\[
\Pr[C = b] = \Pr[M = a] \cdot \Pr[K = 1] + \Pr[M = z] \cdot \Pr[K = 2]
\]
\[
= p \cdot \frac{1}{26} + (1 - p) \cdot \frac{1}{26}
\]
\[
= \frac{1}{26}
\]
Example 3

Consider the shift cipher, and the distribution

\[ \Pr[M = 'one'] = \frac{1}{2}, \Pr[M = 'ten'] = \frac{1}{2} \]

\[ \Pr[C = rqh] = \text{Discuss with Neighbor} \]
Example 3

Consider the shift cipher, and the distribution
\[ \Pr[M = 'one'] = \frac{1}{2}, \Pr[M = 'ten'] = \frac{1}{2} \]

\[ \Pr[C = rqh] = \text{Discuss with Neighbor} \]

\[ \Pr[C = rqh|M = \text{one}] \cdot \Pr[M = \text{one}] + \Pr[C = rqh|M = \text{ten}] \cdot \Pr[M = \text{ten}] \]

\[ = \frac{1}{26} \cdot \frac{1}{2} + 0 \cdot \frac{1}{2} = \frac{1}{52} \]
Example 3

Consider the shift cipher, and the distribution
\[ \Pr[M = \text{'one'}] = \frac{1}{2}, \Pr[M = \text{'ten'}] = \frac{1}{2} \]

\[ \Pr[C = rqh] = \text{Discuss with Neighbor} \]

\[ \Pr[C = rqh|M = \text{one}] \cdot \Pr[M = \text{one}] + \Pr[C = rqh|M = \text{ten}] \cdot \Pr[M = \text{ten}] \]

\[ = \frac{1}{26} \cdot \frac{1}{2} + 0 \cdot \frac{1}{2} = \frac{1}{52} \]

\[ \Pr[C = abc] = \text{Discuss with Neighbor} \]
Example 3

Consider the shift cipher, and the distribution
\[ \Pr[M = 'one'] = \frac{1}{2}, \Pr[M = 'ten'] = \frac{1}{2} \]

\[ \Pr[C = rqh] = \text{Discuss with Neighbor} \]

\[ \Pr[C = rqh|M = one] \cdot \Pr[M = one] + \Pr[C = rqh|M = ten] \cdot \Pr[M = ten] \]

\[ = \frac{1}{26} \cdot \frac{1}{2} + 0 \cdot \frac{1}{2} = \frac{1}{52} \]

\[ \Pr[C = abc] = \text{Discuss with Neighbor} \]

\[ \Pr[C = abc|M = one] \cdot \Pr[M = one] + \Pr[C = abc|M = ten] \cdot \Pr[M = ten] \]

\[ = 0 \cdot \frac{1}{2} + 0 \cdot \frac{1}{2} = 0 \]
Perfect secrecy

Informal: Assume there is a message $m$ such that Eve really cares if the message is $m$. Before Eve sees the ciphertext she knows $\Pr(M = m)$. After Eve sees the ciphertext we want here to not gain any knowledge whatsoever.

Formal: Encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is perfectly secret if for every distribution over $\mathcal{M}$, every $m \in \mathcal{M}$, and every $c \in \mathcal{C}$ with $\Pr[C = c] > 0$, it holds that

$$\Pr[M = m | C = c] = \Pr[M = m]$$

The distribution of $M$ does not change conditioned on observing the ciphertext.
Shift Cipher

Does the Shift Cipher have perfect secrecy? Vote

1. YES
2. NO
3. OTHER
Does the Shift Cipher have perfect secrecy? Vote

1. YES
2. NO
3. OTHER

OTHER- the question is ill defined. Need to know the distribution of messages.
Consider the shift cipher with 1-letter messages and distribution 
\((\forall x)\Pr(M = x) = \frac{1}{26}\).

Need to calculate \(\Pr[M = a | C = d]\).

Need \(\Pr[M = a \land C = d] = \Pr[M = a] \times \Pr[C = d] = \frac{1}{26} \times \frac{1}{26}\)

(If \(M = a\) then the only way \(C = d\) is if \(k = 3\), which happens with \(\Pr \frac{1}{26}\).

\(\Pr[C = d] = \Pr[M = a]Pr[k = 3] + \Pr[M = b]Pr[k = 2] + \ldots + \Pr[M = z]Pr[k = 4] = 26 \times \frac{1}{26} \times \frac{1}{26} = \frac{1}{26}.\)

So

\(\Pr[M = a | C = d] = \frac{\Pr[M = a \land C = d]}{\Pr[C = d]} = (\frac{1}{26})^2 / \frac{1}{26} = \frac{1}{26} = \Pr[M = a]\)

What I did for \(M = a\) and \(C = d\) works for any pair.
Consider the shift cipher with 1-letter messages and distribution \((\forall x)[Pr(M = x) = \frac{1}{26}]\).

Need to calculate \(Pr[M = a | C = d]\).

Need \(Pr[M = a \land C = d] = Pr[M = a] \times Pr[C = d] = \frac{1}{26} \times \frac{1}{26}\) (If \(M = a\) then the only way \(C = d\) is if \(k = 3\), which happens with \(Pr \frac{1}{26}\).)

\(Pr[C = d] = Pr[M = a]Pr[k = 3] + Pr[M = b]Pr[k = 2] + \cdots + Pr[M = z]Pr[k = 4] = 26 \times \frac{1}{26} \times \frac{1}{26} = \frac{1}{26}\).

So

\(Pr[M = a | C = d] = \frac{Pr[M = a \land C = d]}{Pr[C = d]} = \left(\frac{1}{26}\right)^2 / \frac{1}{26} = \frac{1}{26} = Pr[M = a]\)

What I did for \(M = a\) and \(C = d\) works for any pair.

Is this enough to prove that 1-letter Shift is Perfectly Secure?
Discuss with neighbor.
Consider the shift cipher with 1-letter messages and distribution 
\[(\forall x)[\Pr(M = x) = \frac{1}{26}].\]
Need to calculate \(\Pr[M = a | C = d]\).
Need \(\Pr[M = a \land C = d] = \Pr[M = a] \times \Pr[C = d] = \frac{1}{26} \frac{1}{26}\)
(If \(M = a\) then the only way \(C = d\) is if \(k = 3\), which happens with \(\Pr \frac{1}{26}\).)
\(\Pr[C = d] = \Pr[M = a]Pr[k = 3] + \Pr[M = b]Pr[k = 2] + \cdots + \Pr[M = z]Pr[k = 4] = 26 \frac{1}{26} \frac{1}{26} = \frac{1}{26}.\)
So
\(\Pr[M = a | C = d] = \frac{\Pr[M = a \land C = d]}{\Pr[C = d]} = (\frac{1}{26})^2 / \frac{1}{26} = \frac{1}{26} = \Pr[M = a]\)
What I did for \(M = a\) and \(C = d\) works for any pair.
Is this enough to prove that 1-letter Shift is Perfectly Secure?
Discuss with neighbor.
NO- we need this to work for ANY distribution.
Consider the shift cipher with 2-letter messages and distribution

1. \( \Pr[M = ab] = \frac{1}{2} \),
2. \( \Pr[M = cd] = \frac{1}{2} \)

Take \( m = ab \) and \( c = pr \)
\( \Pr[M = ab \mid C = pr] = 0 \neq \Pr[M = ab] \)
Example 5

Consider the shift cipher with 1-letter messages and distribution

1. \( \Pr[M = a'] = \frac{1}{2}, \)
2. \( \Pr[M = 'b'] = \frac{1}{2} \)

Take \( m = 'a' \) and \( c = 'd' \)

\( \Pr[M = 'a' | C = 'd'] = ? \)

Need \( \Pr[M = 'a' \land C = 'd'] = \Pr[M = 'a'] \times \Pr[C = 'd'] = \frac{1}{2} \times \frac{1}{26} \)

(If \( M = 'a' \) then the only way \( C = 'd' \) is if \( k = 3 \), which happens with \( \Pr \frac{1}{26} \).

\( \Pr[C = 'd'] = \Pr[M = a] \times Pr[k = 4] + Pr[M = b] \times Pr[k = 3] = \frac{1}{2} \times \frac{1}{26} + \frac{1}{2} \times \frac{1}{26} = \frac{1}{26} \).

So
Bayes’s theorem

\[ Pr[A|B] = Pr[B|A] \cdot \frac{Pr[A]}{Pr[B]} \]
Example 4

- Shift cipher;
  \[ \Pr[M = 'hi'] = 0.3 \]
  \[ \Pr[M = 'no'] = 0.2 \Pr[M = 'in'] = 0.5 \]

- \[ \Pr[M = 'hi'|C = 'xy'] =? \]
  \[ = \Pr[C = 'xy'|M = 'hi'] \cdot \Pr[M = 'hi']/\Pr[C = 'xy'] \]
Example 4, continued

- $\Pr[C = 'xy' \mid M = 'hi'] = \frac{1}{26}$

- $Pr[C = 'xy']$
  
  $= \Pr[C = 'xy'\mid M = 'hi'] \cdot .3 + \Pr[C = 'xy'\mid M = 'no'] \cdot .2 + \Pr[C = 'xy'\mid M = 'in'] \cdot 0.5$
  
  $= \frac{1}{26} \cdot 0.3 + \frac{1}{26} \cdot 0.2 + 0 \cdot 0.5$
  
  $= \frac{1}{52}$
Example 4, continued

\[
\Pr[C = 'hi' \mid M = 'xy'] = ?
\]

\[
= \Pr[C = 'xy' \mid M = 'hi'] \cdot \frac{\Pr[M = 'hi']}{\Pr[C = 'xy']}
\]

\[
= \frac{1}{26} \cdot \frac{0.3}{\frac{1}{52}}
\]

\[
= 0.6
\]

\[\neq \Pr[M = 'hi']\]
Conclusion

- The shift cipher is not perfectly secret!
  - At least not for 2-character messages
- How to construct a perfectly secret scheme?
One-time pad

- Patented in 1917 by Vernam
  - Recent historical research indicates it was invented (at least) 35 years earlier
- Proven perfectly secret by Shannon (1949)
One-time pad

- Let $\mathcal{M} = \{0, 1\}^n$

- $Gen$: choose a uniform key $k \in \{0, 1\}^n$

- $Enc_k(m) = k \oplus m$

- $Dec_k(c) = k \oplus c$

- Correctness:

$$Dec_k(Enc_k(m)) = k \oplus (k \oplus m)$$

$$= (k \oplus k) \oplus m$$

$$= m$$
One-time pad

- n bits
- key
- n bits
- message
- n bits
- ciphertext