BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

Gen 2-letter Sub and Matrix Codes

October 9, 2021

Shift, Affine, Vig, Gen Sub, Easy to Crack

Shift, Affine, Vig all 1-letter substitutions. Freq cracked them.

Shift, Affine, Vig, Gen Sub, Easy to Crack

Shift, Affine, Vig all 1-letter substitutions. Freq cracked them.
Idea: Lets substitute two letters at a time.

Shift, Affine, Vig, Gen Sub, Easy to Crack

Shift, Affine, Vig all 1-letter substitutions. Freq cracked them.
Idea: Lets substitute two letters at a time.
An Idea Which History Passed By:
Def Gen Sub 2-Cipher with perm f on $\{0, \ldots, 25\}^2$.

Shift, Affine, Vig, Gen Sub, Easy to Crack

Shift, Affine, Vig all 1-letter substitutions. Freq cracked them.
Idea: Lets substitute two letters at a time.
An Idea Which History Passed By:
Def Gen Sub 2-Cipher with perm f on $\{0, \ldots, 25\}^2$.

1. Encrypt via $xy \to f(xy)$.

Shift, Affine, Vig, Gen Sub, Easy to Crack

Shift, Affine, Vig all 1-letter substitutions. Freq cracked them.
Idea: Lets substitute two letters at a time.
An Idea Which History Passed By:
Def Gen Sub 2-Cipher with perm f on $\{0, \ldots, 25\}^2$.

1. Encrypt via $xy \to f(xy)$.
2. Decrypt via $xy \to f^{-1}(xy)$.

Shift, Affine, Vig, Gen Sub, Easy to Crack

Shift, Affine, Vig all 1-letter substitutions. Freq cracked them.
Idea: Lets substitute two letters at a time.
An Idea Which History Passed By:
Def Gen Sub 2-Cipher with perm f on $\{0, \ldots, 25\}^2$.

1. Encrypt via $xy \rightarrow f(xy)$.
2. Decrypt via $xy \rightarrow f^{-1}(xy)$.

Why never used?

Shift, Affine, Vig, Gen Sub, Easy to Crack

Shift, Affine, Vig all 1-letter substitutions. Freq cracked them.
Idea: Lets substitute two letters at a time.
An Idea Which History Passed By:
Def Gen Sub 2-Cipher with perm f on $\{0, \ldots, 25\}^2$.

1. Encrypt via $xy \rightarrow f(xy)$.
2. Decrypt via $xy \rightarrow f^{-1}(xy)$.

Why never used?

1. It was used but they kept it hidden!

Shift, Affine, Vig, Gen Sub, Easy to Crack

Shift, Affine, Vig all 1-letter substitutions. Freq cracked them.
Idea: Lets substitute two letters at a time.
An Idea Which History Passed By:
Def Gen Sub 2-Cipher with perm f on $\{0, \ldots, 25\}^2$.

1. Encrypt via $xy \rightarrow f(xy)$.
2. Decrypt via $xy \rightarrow f^{-1}(xy)$.

Why never used?

1. It was used but they kept it hidden!
2. The key length is roughly $26^2 \times 10 = 6760$ bits.

Shift, Affine, Vig, Gen Sub, Easy to Crack

Shift, Affine, Vig all 1-letter substitutions. Freq cracked them.
Idea: Lets substitute two letters at a time.
An Idea Which History Passed By:
Def Gen Sub 2-Cipher with perm f on $\{0, \ldots, 25\}^2$.

1. Encrypt via $xy \rightarrow f(xy)$.
2. Decrypt via $xy \rightarrow f^{-1}(xy)$.

Why never used?

1. It was used but they kept it hidden!
2. The key length is roughly $26^2 \times 10 = 6760$ bits.
3. There was never a time when it was (a) easy to use, (b) hard to crack, and (c) better ciphers were not known.

Shift, Affine, Vig, Gen Sub, Easy to Crack

Shift, Affine, Vig all 1-letter substitutions. Freq cracked them.
Idea: Lets substitute two letters at a time.
An Idea Which History Passed By:
Def Gen Sub 2-Cipher with perm f on $\{0, \ldots, 25\}^2$.

1. Encrypt via $xy \rightarrow f(xy)$.
2. Decrypt via $xy \rightarrow f^{-1}(xy)$.

Why never used?

1. It was used but they kept it hidden!
2. The key length is roughly $26^2 \times 10 = 6760$ bits.
3. There was never a time when it was (a) easy to use, (b) hard to crack, and (c) better ciphers were not known.

Need bijection of $\{0, \ldots, 25\} \times \{0, \ldots, 25\}$ that is easy to use.

The Matrix Cipher

Def Matrix Cipher. Pick M a 2×2 matrix.

The Matrix Cipher

Def Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \to M(xy)$.

The Matrix Cipher

Def Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \rightarrow M(xy)$.
2. Decrypt via $xy \rightarrow M^{-1}(xy)$.

The Matrix Cipher

Def Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \to M(xy)$.
2. Decrypt via $xy \to M^{-1}(xy)$.

Encode: Break text T into blocks of 2, apply M to each pair.

The Matrix Cipher

Def Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \to M(xy)$.
2. Decrypt via $xy \to M^{-1}(xy)$.

Encode: Break text T into blocks of 2, apply M to each pair.

Decode: Do the same only with M^{-1}.

The Matrix Cipher

Def Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \to M(xy)$.
2. Decrypt via $xy \to M^{-1}(xy)$.

Encode: Break text T into blocks of 2, apply M to each pair.

Decode: Do the same only with M^{-1}.
OH!

The Matrix Cipher

Def Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \to M(xy)$.
2. Decrypt via $xy \to M^{-1}(xy)$.

Encode: Break text T into blocks of 2, apply M to each pair.

Decode: Do the same only with M^{-1}.
OH! is it easy to see if M^{-1} exists? To find M^{-1}?

The Matrix Cipher

Def Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \to M(xy)$.
2. Decrypt via $xy \to M^{-1}(xy)$.

Encode: Break text T into blocks of 2, apply M to each pair.

Decode: Do the same only with M^{-1}.
OH! is it easy to see if M^{-1} exists? To find M^{-1}?

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Then

The Matrix Cipher

Def Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \to M(xy)$.
2. Decrypt via $xy \to M^{-1}(xy)$.

Encode: Break text T into blocks of 2, apply M to each pair.

Decode: Do the same only with M^{-1}.
OH! is it easy to see if M^{-1} exists? To find M^{-1}?

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Then

$$M^{-1} = \frac{1}{ad - bc} \times \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

The Matrix Cipher

Def Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \to M(xy)$.
2. Decrypt via $xy \to M^{-1}(xy)$.

Encode: Break text T into blocks of 2, apply M to each pair.

Decode: Do the same only with M^{-1}.
OH! is it easy to see if M^{-1} exists? To find M^{-1}?

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Then

$$M^{-1} = \frac{1}{ad - bc} \times \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Do you recognize the expression $ad - bc$?

The Matrix Cipher

Def Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \to M(xy)$.
2. Decrypt via $xy \to M^{-1}(xy)$.

Encode: Break text T into blocks of 2, apply M to each pair.

Decode: Do the same only with M^{-1}.
OH! is it easy to see if M^{-1} exists? To find M^{-1}?

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Then

$$M^{-1} = \frac{1}{ad - bc} \times \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Do you recognize the expression $ad - bc$? Determinant!

Inverse Matrix in $\mathbb{C}$ and in Mods

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Inverse Matrix in $\mathbb{C}$ and in Mods

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

1. Matrix M over $\mathbb{C}$ has an inverse iff $ad - bc \neq 0$.

Inverse Matrix in $\mathbb{C}$ and in Mods

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

1. Matrix M over $\mathbb{C}$ has an inverse iff $ad - bc \neq 0$.
2. Matrix M over Mod n has an inverse iff $ad - bc$ is rel prime to n iff $ad - bc$ has an inverse in Mod n.

Inverse Matrix in $\mathbb{C}$ and in Mods

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

1. Matrix M over $\mathbb{C}$ has an inverse iff $ad - bc \neq 0$.
2. Matrix M over Mod n has an inverse iff $ad - bc$ is rel prime to n iff $ad - bc$ has an inverse in Mod n.
3. Matrix M over Mod 26 has an inverse iff $ad - bc$ is rel prime to 26 iff $ad - bc$ has no factors of 2 or 13 iff has an inverse in Mod 26.

The Matrix Cipher

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Good News:

The Matrix Cipher

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Good News:

1. Can test if M^{-1} exists, and if so find it, easily.

The Matrix Cipher

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Good News:

1. Can test if M^{-1} exists, and if so find it, easily.
2. M small, so Key small.

The Matrix Cipher

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Good News:

1. Can test if M^{-1} exists, and if so find it, easily.
2. M small, so Key small.
3. Applying M or M^{-1} to a vector is easy computationally.

The Matrix Cipher

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Good News:

1. Can test if M^{-1} exists, and if so find it, easily.
2. M small, so Key small.
3. Applying M or M^{-1} to a vector is easy computationally.

Bad News:

The Matrix Cipher

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Good News:

1. Can test if M^{-1} exists, and if so find it, easily.
2. M small, so Key small.
3. Applying M or M^{-1} to a vector is easy computationally.

Bad News:

1. Eve **can** crack using frequencies of pairs of letters.

The Matrix Cipher

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Good News:

1. Can test if M^{-1} exists, and if so find it, easily.
2. M small, so Key small.
3. Applying M or M^{-1} to a vector is easy computationally.

Bad News:

1. Eve **can** crack using frequencies of pairs of letters.
2. Eve **can** crack with brute force–Key space $< 26^4 = 456976$. Small.

The Matrix Cipher

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Good News:

1. Can test if M^{-1} exists, and if so find it, easily.
2. M small, so Key small.
3. Applying M or M^{-1} to a vector is easy computationally.

Bad News:

1. Eve **can** crack using frequencies of pairs of letters.
2. Eve **can** crack with brute force–Key space $< 26^4 = 456976$. Small.

So what to do?

The Matrix Cipher

Def Pick $n \in \mathbb{N}$ and M an $\mathbf{n} \times \mathbf{n}$ matrix with det rel prime to 26.

1. Encrypt via $\vec{x} \to M(\vec{x})$.
2. Decrypt via $\vec{y} \to M^{-1}(\vec{y})$

We'll take $n = 8$.

The Matrix Cipher

Def Pick $n \in \mathbb{N}$ and M an $\mathbf{n} \times \mathbf{n}$ matrix with det rel prime to 26.

1. Encrypt via $\vec{x} \to M(\vec{x})$.
2. Decrypt via $\vec{y} \to M^{-1}(\vec{y})$

We'll take $n = 8$.

1. M still small, so Key small.

The Matrix Cipher

Def Pick $n \in \mathbb{N}$ and M an $\mathbf{n} \times \mathbf{n}$ matrix with det rel prime to 26.

1. Encrypt via $\vec{x} \to M(\vec{x})$.
2. Decrypt via $\vec{y} \to M^{-1}(\vec{y})$

We'll take $n = 8$.

1. M still small, so Key small.
2. Finding M^{-1}, mult by M or M^{-1} fast.

The Matrix Cipher

Def Pick $n \in \mathbb{N}$ and M an $\mathbf{n} \times \mathbf{n}$ matrix with det rel prime to 26.

1. Encrypt via $\vec{x} \to M(\vec{x})$.
2. Decrypt via $\vec{y} \to M^{-1}(\vec{y})$

We'll take $n = 8$.

1. M still small, so Key small.
2. Finding M^{-1}, mult by M or M^{-1} fast.
3. Eve **cannot** use brute force. Key Space is $\sim 26^{64} \sim 10^{90}$, Number of protons is $\sim 10^{79}$. (the number of non-invertible matrices is very small so 26^{64} is a good approximation).

Lets Try Brute Force Even if Slow

Lets Try Brute Force Even if Slow

1. Input T, a coded text.

Lets Try Brute Force Even if Slow

1. Input T, a coded text.
2. For **every** 8×8 matrix M over $\mathbb{Z}_{26}$,

Lets Try Brute Force Even if Slow

1. Input T, a coded text.
2. For **every** 8×8 matrix M over $\mathbb{Z}_{26}$,
    2.1 Test if M is invertible. If not then goto next matrix.

Lets Try Brute Force Even if Slow

1. Input T, a coded text.
2. For **every** 8×8 matrix M over $\mathbb{Z}_{26}$,
   2.1 Test if M is invertible. If not then goto next matrix.
   2.2 Decode T into T' using M.

Lets Try Brute Force Even if Slow

1. Input T, a coded text.
2. For **every** 8×8 matrix M over $\mathbb{Z}_{26}$,
   2.1 Test if M is invertible. If not then goto next matrix.
   2.2 Decode T into T' using M.
   2.3 IF IS-ENGLISH(T')=YES then STOP and output T', else goto next matrix M.

Lets Try Brute Force Even if Slow

1. Input T, a coded text.
2. For **every** 8×8 matrix M over $\mathbb{Z}_{26}$,
    2.1 Test if M is invertible. If not then goto next matrix.
    2.2 Decode T into T' using M.
    2.3 IF IS-ENGLISH(T')=YES then STOP and output T', else goto next matrix M.

Takes roughly 26^{64} steps.

Can We Do Better?

Takes roughly 26^{64} steps.

Can We Do Better?

Takes roughly 26^{64} steps.

Can we do better?

Can We Do Better?

Takes roughly 26^{64} steps.

Can we do better?

Need to refine the question.

Can We Do Better?

Takes roughly 26^{64} steps.

Can we do better?

Need to refine the question.

Assume T is long and in normal English.

Can We Do Better?

Takes roughly 26^{64} steps.

Can we do better?

Need to refine the question.

Assume T is long and in normal English.

Assume Eve only has access to the ciphertext. VOTE:

Can We Do Better?

Takes roughly 26^{64} steps.

Can we do better?

Need to refine the question.

Assume T is long and in normal English.

Assume Eve only has access to the ciphertext. VOTE:

1. **Yes** There is a clever way to do much better than 26^{64}.

Can We Do Better?

Takes roughly 26^{64} steps.

Can we do better?

Need to refine the question.

Assume T is long and in normal English.

Assume Eve only has access to the ciphertext. VOTE:

1. **Yes** There is a clever way to do much better than 26^{64}.
2. **No** and we can PROVE we can't do better with ciphertext-only.

Can We Do Better?

Takes roughly 26^{64} steps.

Can we do better?

Need to refine the question.

Assume T is long and in normal English.

Assume Eve only has access to the ciphertext. VOTE:

1. **Yes** There is a clever way to do much better than 26^{64}.
2. **No** and we can PROVE we can't do better with ciphertext-only.
3. **Unknown to Science** if we can do better with ciphertext-only.

Can We Do Better?

Takes roughly 26^{64} steps.

Can we do better?

Need to refine the question.

Assume T is long and in normal English.

Assume Eve only has access to the ciphertext. VOTE:

1. **Yes** There is a clever way to do much better than 26^{64}.
2. **No** and we can PROVE we can't do better with ciphertext-only.
3. **Unknown to Science** if we can do better with ciphertext-only.

Yes. We can crack in time 8×26^{8}.

Can Crack in 8×26^8

The attack in the last slide went through every **Matrix**.

Can Crack in 8×26^8

The attack in the last slide went through every **Matrix**.
Better Idea: We take life **one row at a time**.

Can Crack in 8×26^8

The attack in the last slide went through every **Matrix**.
Better Idea: We take life **one row at a time**.
Example: 3×3 matrix cipher. Decode Matrix M.

$$T = t_1 t_2 \cdots t_N \text{ each } t_i \text{ is 3-long}$$

Can Crack in 8×26^8

The attack in the last slide went through every **Matrix**.
Better Idea: We take life **one row at a time**.
Example: 3×3 matrix cipher. Decode Matrix M.

$$T = t_1 t_2 \cdots t_N \text{ each } t_i \text{ is 3-long}$$

Guess the first row of M. Say:

$$\begin{pmatrix} 1 & 1 & 7 \\ * & * & * \\ * & * & * \end{pmatrix}$$

Can Crack in 8×26^8

The attack in the last slide went through every **Matrix**.
Better Idea: We take life **one row at a time**.
Example: 3×3 matrix cipher. Decode Matrix M.

$$T = t_1 t_2 \cdots t_N \text{ each } t_i \text{ is 3-long}$$

Guess the first row of M. Say:

$$\begin{pmatrix} 1 & 1 & 7 \\ * & * & * \\ * & * & * \end{pmatrix}$$

Let $Mt_i = m_i$. Then $(1, 1, 7) \cdot t_i = m_i^1$ is first letter of m_i.

Can Crack in 8×26^8

The attack in the last slide went through every **Matrix**.
Better Idea: We take life **one row at a time**.
Example: 3×3 matrix cipher. Decode Matrix M.

$$T = t_1 t_2 \cdots t_N \text{ each } t_i \text{ is 3-long}$$

Guess the first row of M. Say:

$$\begin{pmatrix} 1 & 1 & 7 \\ * & * & * \\ * & * & * \end{pmatrix}$$

Let $Mt_i = m_i$. Then $(1,1,7) \cdot t_i = m_i^1$ is first letter of m_i.

$$(m_1^1, m_2^1, m_3^1, \ldots, m_N^1)$$

is every third letter.

Can Crack in 8×26^8

The attack in the last slide went through every **Matrix**.
Better Idea: We take life **one row at a time**.
Example: 3×3 matrix cipher. Decode Matrix M.

$$T = t_1 t_2 \cdots t_N \text{ each } t_i \text{ is 3-long}$$

Guess the first row of M. Say:

$$\begin{pmatrix} 1 & 1 & 7 \\ * & * & * \\ * & * & * \end{pmatrix}$$

Let $Mt_i = m_i$. Then $(1,1,7) \cdot t_i = m_i^1$ is first letter of m_i.

$$(m_1^1, m_2^1, m_3^1, \ldots, m_N^1)$$

is every third letter. Can do IS-ENGLISH on it.

Can Crack in 8×26^8

Eve knows that Alice and Bob decode with 8×8 Matrix M.
Ciphertext is

$$T = t_1 t_2 \cdots t_N \qquad t_i = t_i^1 \cdots t_i^8$$

Can Crack in 8×26^8

Eve knows that Alice and Bob decode with 8×8 Matrix M.
Ciphertext is

$$T = t_1 t_2 \cdots t_N \qquad t_i = t_i^1 \cdots t_i^8$$

For $i = 1$ to 8

Can Crack in 8×26^8

Eve knows that Alice and Bob decode with 8×8 Matrix M.
Ciphertext is

$$T = t_1 t_2 \cdots t_N \qquad t_i = t_i^1 \cdots t_i^8$$

For $i = 1$ to 8

For all $r \in \mathbb{Z}_{26}^8$ (guess that r is ith row of B).

Can Crack in 8×26^8

Eve knows that Alice and Bob decode with 8×8 Matrix M.
Ciphertext is

$$T = t_1 t_2 \cdots t_N \qquad t_i = t_i^1 \cdots t_i^8$$

For $i = 1$ to 8

For all $r \in \mathbb{Z}_{26}^8$ (guess that r is ith row of B).

$T' = (r \cdot t_1, \ldots, r \cdot t_N)$ (Is every 8th letter.)

Can Crack in 8×26^8

Eve knows that Alice and Bob decode with 8×8 Matrix M. Ciphertext is

$$T = t_1 t_2 \cdots t_N \qquad t_i = t_i^1 \cdots t_i^8$$

For $i = 1$ to 8

- For all $r \in \mathbb{Z}_{26}^8$ (guess that r is ith row of B).
  - $T' = (r \cdot t_1, \ldots, r \cdot t_N)$ (Is every 8th letter.)
  - IF IS-ENGLISH(T')=YES then $r_i = r$ and goto next i. Else goto the next r.

Can Crack in 8×26^8

Eve knows that Alice and Bob decode with 8×8 Matrix M.
Ciphertext is

$$T = t_1 t_2 \cdots t_N \qquad t_i = t_i^1 \cdots t_i^8$$

For $i = 1$ to 8

For all $r \in \mathbb{Z}_{26}^8$ (guess that r is ith row of B).

$T' = (r \cdot t_1, \ldots, r \cdot t_N)$ (Is every 8th letter.)

IF IS-ENGLISH(T')=YES then $r_i = r$ and goto next i. Else goto the next r.

M is

$$\begin{pmatrix} \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots \\ r_1 & \cdots & r_n \\ \vdots & \vdots & \vdots \\ \cdots & \cdots & \cdots \end{pmatrix}$$

Can Crack in 8×26^8

Eve knows that Alice and Bob decode with 8×8 Matrix M.
Ciphertext is

$$T = t_1 t_2 \cdots t_N \qquad t_i = t_i^1 \cdots t_i^8$$

For $i = 1$ to 8

For all $r \in \mathbb{Z}_{26}^8$ (guess that r is ith row of B).

$T' = (r \cdot t_1, \ldots, r \cdot t_N)$ (Is every 8th letter.)

IF IS-ENGLISH(T')=YES then $r_i = r$ and goto next i. Else goto the next r.

M is

$$\begin{pmatrix} \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots \\ r_1 & \cdots & r_n \\ \vdots & \vdots & \vdots \\ \cdots & \cdots & \cdots \end{pmatrix}$$

Takes 8×26^8 steps.

More General n

If M is $n \times n$ matrix.

More General n

If M is $n \times n$ matrix.

Brute force takes $O(26^{n^2})$.

More General n

If M is $n \times n$ matrix.

Brute force takes $O(26^{n^2})$.

The row-by-row method takes $O(n26^n)$.

Important Lesson

Assume: 26^{64} time is big enough to thwart Eve.

Important Lesson

Assume: 26^{64} time is big enough to thwart Eve.

1. If we think that best Eve can do is $O(26^{n^2})$ then we take $n = 8$, so Eve needs $O(26^{64})$.

Important Lesson

Assume: 26^{64} time is big enough to thwart Eve.

1. If we think that best Eve can do is $O(26^{n^2})$ then we take $n = 8$, so Eve needs $O(26^{64})$.
2. If we think that best Eve can do is $O(n26^n)$ then we take $n = 80$, so Eve needs $O(80 \times 26^{80})$.

Important Lesson

Assume: 26^{64} time is big enough to thwart Eve.

1. If we think that best Eve can do is $O(26^{n^2})$ then we take $n = 8$, so Eve needs $O(26^{64})$.
2. If we think that best Eve can do is $O(n26^n)$ then we take $n = 80$, so Eve needs $O(80 \times 26^{80})$.
3. There may be a period of time when Eve knows the technique that Alice and Bob do not know that she knows, so for that time she can crack.

Important Lesson

Assume: 26^{64} time is big enough to thwart Eve.

1. If we think that best Eve can do is $O(26^{n^2})$ then we take $n = 8$, so Eve needs $O(26^{64})$.
2. If we think that best Eve can do is $O(n26^n)$ then we take $n = 80$, so Eve needs $O(80 \times 26^{80})$.
3. There may be a period of time when Eve knows the technique that Alice and Bob do not know that she knows, so for that time she can crack.
4. After Alice and Bob learn the technique they have to up their parameters. This is a mild win for Eve in that A and B have to work harder.

The History of Cryptography in One Slide

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 8$).

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 8$).
2. Alice and Bob think it's uncrackable and have a "proof" that it is uncrackable (e.g., Eve HAS to go through all 26^{64} matrices).

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 8$).
2. Alice and Bob think it's uncrackable and have a "proof" that it is uncrackable (e.g., Eve HAS to go through all 26^{64} matrices).
3. Eve Cracks it. (The trick above- only about 8×26^{8}.)

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 8$).
2. Alice and Bob think it's uncrackable and have a "proof" that it is uncrackable (e.g., Eve HAS to go through all 26^{64} matrices).
3. Eve Cracks it. (The trick above- only about 8×26^8.)
4. Lather, Rinse, Repeat.

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 8$).
2. Alice and Bob think it's uncrackable and have a "proof" that it is uncrackable (e.g., Eve HAS to go through all 26^{64} matrices).
3. Eve Cracks it. (The trick above- only about 8×26^8.)
4. Lather, Rinse, Repeat.

Above attack on Matrix Cipher is a microcosm of this history.

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 8$).
2. Alice and Bob think it's uncrackable and have a "proof" that it is uncrackable (e.g., Eve HAS to go through all 26^{64} matrices).
3. Eve Cracks it. (The trick above- only about 8×26^8.)
4. Lather, Rinse, Repeat.

Above attack on Matrix Cipher is a microcosm of this history.

Proofs rely on limiting what Eve can do, and hence do not work if Eve does something else.

Is Matrix Cipher with n Large Crackable?

Assume Alice and Bob are using the Matrix Cipher with n large (80 is large enough).

Is Matrix Cipher with n Large Crackable?

Assume Alice and Bob are using the Matrix Cipher with n large (80 is large enough).

Alice and Bob **can** handle matrices of this size easily

Is Matrix Cipher with n Large Crackable?

Assume Alice and Bob are using the Matrix Cipher with n large (80 is large enough).

Alice and Bob **can** handle matrices of this size easily

Is Matrix Cipher with $n = 80$ secure?

Is Matrix Cipher with n Large Crackable?

Assume Alice and Bob are using the Matrix Cipher with n large (80 is large enough).

Alice and Bob **can** handle matrices of this size easily

Is Matrix Cipher with $n = 80$ secure?

Have to ask this carefully.

Is Matrix Cipher with n Large Crackable?

Assume Alice and Bob are using the Matrix Cipher with n large (80 is large enough).

Alice and Bob **can** handle matrices of this size easily

Is Matrix Cipher with $n = 80$ secure?

Have to ask this carefully.

1. Plaintext is a very long text of normal English.

Is Matrix Cipher with n Large Crackable?

Assume Alice and Bob are using the Matrix Cipher with n large (80 is large enough).

Alice and Bob **can** handle matrices of this size easily

Is Matrix Cipher with $n = 80$ secure?

Have to ask this carefully.

1. Plaintext is a very long text of normal English.
2. Eve sees the entire ciphertext T.

Is Matrix Cipher with n Large Crackable?

Assume Alice and Bob are using the Matrix Cipher with n large (80 is large enough).

Alice and Bob **can** handle matrices of this size easily

Is Matrix Cipher with $n = 80$ secure?

Have to ask this carefully.

1. Plaintext is a very long text of normal English.
2. Eve sees the entire ciphertext T.
3. Eve has access to frequency tables for 1,2,...,80 long blocks of letters.

Is Matrix Cipher with n Large Crackable?

Assume Alice and Bob are using the Matrix Cipher with n large (80 is large enough).

Alice and Bob **can** handle matrices of this size easily

Is Matrix Cipher with $n = 80$ secure?

Have to ask this carefully.

1. Plaintext is a very long text of normal English.
2. Eve sees the entire ciphertext T.
3. Eve has access to frequency tables for 1,2,. . .,80 long blocks of letters.

Can Eve decode T?

Is Matrix Cipher with n Large Crackable?

Assume Alice and Bob are using the Matrix Cipher with n large (80 is large enough).

Alice and Bob **can** handle matrices of this size easily

Is Matrix Cipher with $n = 80$ secure?

Have to ask this carefully.

1. Plaintext is a very long text of normal English.
2. Eve sees the entire ciphertext T.
3. Eve has access to frequency tables for 1,2,. . .,80 long blocks of letters.

Can Eve decode T? Vote

Is Matrix Cipher with n Large Crackable?

Assume Alice and Bob are using the Matrix Cipher with n large (80 is large enough).

Alice and Bob **can** handle matrices of this size easily

Is Matrix Cipher with $n = 80$ secure?

Have to ask this carefully.

1. Plaintext is a very long text of normal English.
2. Eve sees the entire ciphertext T.
3. Eve has access to frequency tables for 1,2,...,80 long blocks of letters.

Can Eve decode T? Vote

- **Yes** Eve can find the plaintext (or most of it).

Is Matrix Cipher with n Large Crackable?

Assume Alice and Bob are using the Matrix Cipher with n large (80 is large enough).

Alice and Bob **can** handle matrices of this size easily

Is Matrix Cipher with $n = 80$ secure?

Have to ask this carefully.

1. Plaintext is a very long text of normal English.
2. Eve sees the entire ciphertext T.
3. Eve has access to frequency tables for 1,2,...,80 long blocks of letters.

Can Eve decode T? Vote

- **Yes** Eve can find the plaintext (or most of it).
- **No** One can prove that Eve cannot find the plaintext.

Is Matrix Cipher with n Large Crackable?

Assume Alice and Bob are using the Matrix Cipher with n large (80 is large enough).

Alice and Bob **can** handle matrices of this size easily

Is Matrix Cipher with $n = 80$ secure?

Have to ask this carefully.

1. Plaintext is a very long text of normal English.
2. Eve sees the entire ciphertext T.
3. Eve has access to frequency tables for 1,2,...,80 long blocks of letters.

Can Eve decode T? Vote

- **Yes** Eve can find the plaintext (or most of it).
- **No** One can prove that Eve cannot find the plaintext.
- **Unknown to Science!** (Hmmm—the NSA might know and is not telling.)

Is Matrix Cipher with n Large Crackable?

Assume Alice and Bob are using the Matrix Cipher with n large (80 is large enough).

Alice and Bob **can** handle matrices of this size easily

Is Matrix Cipher with $n = 80$ secure?

Have to ask this carefully.

1. Plaintext is a very long text of normal English.
2. Eve sees the entire ciphertext T.
3. Eve has access to frequency tables for 1,2,...,80 long blocks of letters.

Can Eve decode T? Vote

- **Yes** Eve can find the plaintext (or most of it).
- **No** One can prove that Eve cannot find the plaintext.
- **Unknown to Science!** (Hmmm—the NSA might know and is not telling.)

Answer Unknown to Science.

Is Matrix Cipher with n Large Crackable?

Assume Alice and Bob are using the Matrix Cipher with n large (80 is large enough).

Alice and Bob **can** handle matrices of this size easily

Is Matrix Cipher with $n = 80$ secure?

Have to ask this carefully.

1. Plaintext is a very long text of normal English.
2. Eve sees the entire ciphertext T.
3. Eve has access to frequency tables for 1,2,...,80 long blocks of letters.

Can Eve decode T? Vote

- **Yes** Eve can find the plaintext (or most of it).
- **No** One can prove that Eve cannot find the plaintext.
- **Unknown to Science!** (Hmmm—the NSA might know and is not telling.)

Answer Unknown to Science.

Question How come Matrix cipher is not used? Discuss.

Is Matrix Cipher with n Large Crackable?

In our vote we assumed

Is Matrix Cipher with n Large Crackable?

In our vote we assumed

Eve only has access to ciphertext

Is Matrix Cipher with n Large Crackable?

In our vote we assumed

Eve only has access to ciphertext

In reality

Is Matrix Cipher with n Large Crackable?

In our vote we assumed

Eve only has access to ciphertext

In reality

Eve has much more information.

Is Matrix Cipher with n Large Crackable?

In our vote we assumed

Eve only has access to ciphertext

In reality

Eve has much more information.

Eve will have old messages and what they decoded to.

Example of What Eve Might Know

Scenario:

Example of What Eve Might Know

Scenario:

1. Eve knows that Alice is telling Bob the initials of the city she will be in next week.

Example of What Eve Might Know

Scenario:

1. Eve knows that Alice is telling Bob the initials of the city she will be in next week.
2. Eve intercepts the message. It is (3,9).

Example of What Eve Might Know

Scenario:

1. Eve knows that Alice is telling Bob the initials of the city she will be in next week.
2. Eve intercepts the message. It is (3,9).
3. Eve is NOT able to crack this.

Example of What Eve Might Know

Scenario:

1. Eve knows that Alice is telling Bob the initials of the city she will be in next week.
2. Eve intercepts the message. It is (3,9).
3. Eve is NOT able to crack this.
4. The next day Eve follows Alice and sees that she goes to New York. NY is (13,24).

Example of What Eve Might Know

Scenario:

1. Eve knows that Alice is telling Bob the initials of the city she will be in next week.
2. Eve intercepts the message. It is (3,9).
3. Eve is NOT able to crack this.
4. The next day Eve follows Alice and sees that she goes to New York. NY is (13,24).
5. Eve knows that $(3,9) = M(13,24)$.

Cracking Matrix Cipher

Example using 2×2 Matrix Cipher.
Eve learns that (13,24) encrypts to $(3, 9)$. Hence:

Cracking Matrix Cipher

Example using 2×2 Matrix Cipher.
Eve learns that (13,24) encrypts to $(3, 9)$. Hence:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 13 \\ 24 \end{pmatrix} = \begin{pmatrix} 3 \\ 9 \end{pmatrix}$$

Cracking Matrix Cipher

Example using 2×2 Matrix Cipher.
Eve learns that (13,24) encrypts to $(3, 9)$. Hence:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 13 \\ 24 \end{pmatrix} = \begin{pmatrix} 3 \\ 9 \end{pmatrix}$$

So

$$\begin{aligned} 13a + 24b &= 3 \\ 13c + 24d &= 9 \end{aligned}$$

Two linear equations, Four variables

Cracking Matrix Cipher

Example using 2×2 Matrix Cipher.
Eve learns that (13,24) encrypts to $(3, 9)$. Hence:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 13 \\ 24 \end{pmatrix} = \begin{pmatrix} 3 \\ 9 \end{pmatrix}$$

So

$$\begin{aligned} 13a + 24b &= 3 \\ 13c + 24d &= 9 \end{aligned}$$

Two linear equations, Four variables

If Eve learns one more 2-letter message decoding then she will have

Four linear equations, Four variables

which she can solve!

Cracking Matrix Cipher

Example using 2×2 Matrix Cipher.
Eve learns that (13,24) encrypts to $(3, 9)$. Hence:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 13 \\ 24 \end{pmatrix} = \begin{pmatrix} 3 \\ 9 \end{pmatrix}$$

So

$$\begin{aligned} 13a + 24b &= 3 \\ 13c + 24d &= 9 \end{aligned}$$

Two linear equations, Four variables

If Eve learns one more 2-letter message decoding then she will have

Four linear equations, Four variables

which she can solve! Yeah?

Cracking Matrix Cipher

Example using 2×2 Matrix Cipher.
Eve learns that (13,24) encrypts to $(3, 9)$. Hence:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 13 \\ 24 \end{pmatrix} = \begin{pmatrix} 3 \\ 9 \end{pmatrix}$$

So

$$\begin{aligned} 13a + 24b &= 3 \\ 13c + 24d &= 9 \end{aligned}$$

Two linear equations, Four variables

If Eve learns one more 2-letter message decoding then she will have

Four linear equations, Four variables

which she can solve! Yeah?Boo?

Cracking Matrix Cipher

Example using 2×2 Matrix Cipher.
Eve learns that (13,24) encrypts to $(3, 9)$. Hence:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 13 \\ 24 \end{pmatrix} = \begin{pmatrix} 3 \\ 9 \end{pmatrix}$$

So

$$\begin{aligned} 13a + 24b &= 3 \\ 13c + 24d &= 9 \end{aligned}$$

Two linear equations, Four variables

If Eve learns one more 2-letter message decoding then she will have

Four linear equations, Four variables

which she can solve! Yeah?Boo?Depends whose side you are on.

Upshot

Upshot

1. Matrix Cipher with ciphertext only might be hard to crack.

Upshot

1. Matrix Cipher with ciphertext only might be hard to crack.
2. Matrix Cipher where Eve has access to prior messages is easy to crack.

Upshot

1. Matrix Cipher with ciphertext only might be hard to crack.
2. Matrix Cipher where Eve has access to prior messages is easy to crack.
3. We need to better refine our notion of **attack**.

Upshot

1. Matrix Cipher with ciphertext only might be hard to crack.
2. Matrix Cipher where Eve has access to prior messages is easy to crack.
3. We need to better refine our notion of **attack**.
4. We will do this in a later slide packet.