Cryptocomplexity I

Kryptokomplexität I

Wintersemester 2023/2024

Chapter 2: Some Classical Cryptosystems and Their Cryptanalysis

Dozent: Prof. Dr. J. Rothe

Block Cipher and Substitution Cipher

Definition

- A *block cipher* is a cryptosystem in which both the plaintext space and the ciphertext space is Σ^n, the set of length n strings over some alphabet Σ. The number n is called the *block length* (or sometimes the *period*) of the system.
- A *substitution cipher* is a block cipher with block length one.

Observation:

The encryption functions of a block cipher are permutations.

Because every encryption function has some corresponding decryption function, the encryption functions of a block cipher are injective, and an injective function mapping from Σ^n onto Σ^n is a bijection.

Block Cipher and Substitution Cipher

By this observation, the most general block cipher can be described as follows:

- Fix an alphabet Σ and a block length n, and define the message space and ciphertext space by $M = C = \Sigma^n$.
- Let the key space K be given by the set of all permutations of Σ^n.
- For each key $\pi \in K$, the encryption function E_π and the decryption function D_π, which both map from Σ^n to Σ^n, are defined by:

$$\begin{array}{rcl} E_\pi(\vec{x}) & = & \pi(\vec{x}); \\ D_\pi(\vec{y}) & = & \pi^{-1}(\vec{y}), \end{array}$$

where π^{-1} is the inverse permutation.

Block Cipher and Substitution Cipher

However, this cryptosystem is *impracticable*, since one needs the permutation π to decrypt the message.

Representing $\pi \in K$ by a table containing $\pi(\vec{x})$ for each $\vec{x} \in \Sigma^n$, one obtains a table of size m^n.

That is why it is more reasonable to use only those permutations that result from interchanging the position of cleartext letters.

This is the *permutation cipher*, also known as the *transposition cipher*.

Permutation Cipher, a.k.a. Transposition Cipher

- Let Σ be some alphabet, and let $n \in \mathbb{N}$ be the block length.

- Let $M = C = \Sigma^n$, and let the key space $K = \mathfrak{S}_n$ be the permutation group on n elements.

- For each key $\pi \in \mathfrak{S}_n$, the encryption function E_π and the decryption function D_π, which both map from Σ^n to Σ^n, are defined by:

$$\begin{array}{rcl} E_\pi(x_1 x_2 \cdots x_n) & = & x_{\pi(1)} x_{\pi(2)} \cdots x_{\pi(n)}; \\ D_\pi(y_1 y_2 \cdots y_n) & = & y_{\pi^{-1}(1)} y_{\pi^{-1}(2)} \cdots y_{\pi^{-1}(n)}. \end{array}$$

- Here, the key space has $n!$ elements, and every key can be encoded by a sequence of n numbers.

Arithmetics in $\mathbb{Z}_k$

- Let $k \in \mathbb{N}_+$ and $x, y, z \in \mathbb{Z}$. The number *x is congruent to y modulo k* ($x \equiv y \bmod k$, for short) if and only if k divides the difference $y - x$. For example, $-3 \equiv 16 \bmod 19$ and $8 \equiv 0 \bmod 2$.

- The congruence $\equiv$ modulo k defines an *equivalence relation* on $\mathbb{Z}$, i.e., it is
  - *reflexive* ($x \equiv x \bmod k$),
  - *symmetric* ($x \equiv y \bmod k$ implies $y \equiv x \bmod k$), and
  - *transitive* (if $x \equiv y \bmod k$ and $y \equiv z \bmod k$, then $x \equiv z \bmod k$).

- The set $x + k\mathbb{Z} = \{y \in \mathbb{Z} \mid y \equiv x \bmod k\}$ is said to be the *remainder class of x mod k*. For example, the remainder class of 3 mod 7 is

$$3 + 7\mathbb{Z} = \{3, 3 \pm 7, 3 \pm 2 \cdot 7, \ldots\} = \{3, 10, -4, 17, -11, \ldots\}.$$

Arithmetics in $\mathbb{Z}_k$

- We always choose the smallest natural number in $x + k\mathbb{Z}$ to *represent* the remainder class of x mod k; e.g., 3 represents the class 3 mod 7.
- The set of all remainder classes modulo k is $\mathbb{Z}_k = \{0, 1, \ldots, k-1\}$.
- On $\mathbb{Z}_k$, define the
  - *addition modulo k* by $(x + k\mathbb{Z}) + (y + k\mathbb{Z}) = (x + y) + k\mathbb{Z}$ and the
  - *multiplication modulo k* by $(x + k\mathbb{Z}) \cdot (y + k\mathbb{Z}) = (x \cdot y) + k\mathbb{Z}$.

  For example, in the arithmetics modulo 7, we have

$$\begin{aligned} (3 + 7\mathbb{Z}) + (6 + 7\mathbb{Z}) &= (3 + 6) + 7\mathbb{Z} = 2 + 7\mathbb{Z} \\ (3 + 7\mathbb{Z}) \cdot (4 + 7\mathbb{Z}) &= (3 \cdot 4) + 7\mathbb{Z} = 5 + 7\mathbb{Z}. \end{aligned}$$

Shift Cipher

- The shift cipher is a monoalphabetic symmetric cryptosystem.
  Let $K = M = C = \mathbb{Z}_{26}$.

- The *shift cipher* encrypts messages by shifting (modulo 26) each character of the plaintext by the same number k of letters in the alphabet, where $k \in \mathbb{Z}_{26}$ is the key. Shifting each character of the ciphertext back using the same key k reveals the original message.

- For each key $k \in \mathbb{Z}_{26}$, the encryption function E_k and the decryption function D_k, which both map from $\mathbb{Z}_{26}$ to $\mathbb{Z}_{26}$, are defined by:

$$\begin{aligned} E_k(x) &= (x + k) \bmod 26; \\ D_k(y) &= (y - k) \bmod 26. \end{aligned}$$

Shift Cipher

Example

If we choose the key $k = 17 = \mathrm{R}$, the message

"BRUTUS FORCE EASILY BREAKS CAESAR"

is encrypted as follows:

m	B R U T U S F O R C E E A S I L Y B R E A K S C A E S A R
c	S I L K L J W F I T V V R J Z C P S I V R B J T R V J R I

Table: Example of an encryption by the shift cipher with key $k = 17$

Affine Cipher

- The affine cipher is a monoalphabetic symmetric cryptosystem. Let $M = C = \mathbb{Z}_{26}$ and $K = \{(a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} \,|\, \texttt{gcd}(a,26) = 1\}$.
- The *affine cipher* encrypts messages letter by letter. For each key $(a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$ with $\texttt{gcd}(a,26) = 1$, the encryption function $E_{(a,b)}$ and the decryption function $D_{(a^{-1},b)}$, which both map from $\mathbb{Z}_{26}$ to $\mathbb{Z}_{26}$, are defined by:

$$\begin{aligned} E_{(a,b)}(x) &= ax + b \bmod 26; \\ D_{(a^{-1},b)}(y) &= a^{-1}(y-b) \bmod 26, \end{aligned}$$

where a^{-1} is the inverse element of a in $\mathbb{Z}_{26}$, i.e., $aa^{-1} \equiv a^{-1}a \equiv 1 \bmod 26$. Note that a^{-1} can easily be determined by the *extended algorithm of Euclid*.

Greatest Common Divisor and Euclidian Algorithm

Definition

The *greatest common divisor* ($\mathtt{gcd}(m,n)$) of two given integers m and n is the greatest number $k \in \mathbb{N}$ for which there are numbers $a, b \in \mathbb{Z}$ with $m = a \cdot k$ and $n = b \cdot k$.

```
$\textsc{Euclid}(n, m)$ {
    (* $m$ and $n$ are integers with $m \leq n$ *)
    if $(m = 0)$ return $n$;
        else return $\textsc{Euclid}(m, n \bmod m)$;
}
```

Figure: Computing $\mathtt{gcd}(m,n)$ by the Euclidian Algorithm

Greatest Common Divisor and Euclidian Algorithm

Example: What is the greatest common divisor of $n = 170$ and $m = 102$?

n	m	$n \bmod m$
170	102	68
102	68	34
68	34	0
34	0	

Table: Test run of the Euclidean Algorithm

The algorithm indeed computes the correct solution, since $\texttt{gcd}(170, 102) = 34$ because $3 \cdot 34 = 102$ and $5 \cdot 34 = 170$.

Extended Euclidian Algorithm

```
Extended-Euclid($n, m$) {
    (* $m$ and $n$ are integers with $m \leq n$ *)
    if ($m = 0$) return ($n, 1, 0$);
        else {
            ($g, x', y'$) := Extended-Euclid($m, n \bmod m$);
            $x := y'$;
            $y := x' - y' * \left\lfloor \frac{n}{m} \right\rfloor$;
            return ($g, x, y$);
        }
}
```

Figure: Extended Euclidean Algorithm

Extended Euclidian Algorithm

Example: What is the greatest common divisor of $n = 170$ and $m = 102$?

n	m	g	x	y	Remark

Table: Test run of the extended Euclidean Algorithm

Extended Euclidian Algorithm

Example: What is the greatest common divisor of $n = 170$ and $m = 102$?

n	m	g	x	y	Remark

Table: Test run of the extended Euclidean Algorithm

Extended Euclidian Algorithm

Example: What is the greatest common divisor of $n = 170$ and $m = 102$?

n	m	g	x	y	Remark
170	102				

Table: Test run of the extended Euclidean Algorithm

Extended Euclidian Algorithm

Example: What is the greatest common divisor of $n = 170$ and $m = 102$?

n	m	g	x	y	Remark
170	102				
102	68				

Table: Test run of the extended Euclidean Algorithm

Extended Euclidian Algorithm

Example: What is the greatest common divisor of $n = 170$ and $m = 102$?

n	m	g	x	y	Remark
170	102				
102	68				
68	34				

Table: Test run of the extended Euclidean Algorithm

Extended Euclidian Algorithm

Example: What is the greatest common divisor of $n = 170$ and $m = 102$?

n	m	g	x	y	Remark
170	102				
102	68				
68	34				
34	0	34	1	0	`if` $(m = 0)$ `return` $(n, 1, 0)$

Table: Test run of the extended Euclidean Algorithm

Extended Euclidian Algorithm

Example: What is the greatest common divisor of $n = 170$ and $m = 102$?

n	m	g	x	y	Remark
170	102				
102	68				
68	34	34	0	1	$x := y'; \quad y := x' - y' * \left\lfloor \frac{n}{m} \right\rfloor$
34	0	34	1	0	$\texttt{if}\ (m = 0)\ \texttt{return}\ (n, 1, 0)$

Table: Test run of the extended Euclidean Algorithm

Extended Euclidian Algorithm

Example: What is the greatest common divisor of $n = 170$ and $m = 102$?

n	m	g	x	y	Remark
170	102				
102	68	34	1	-1	
68	34	34	0	1	$x := y'; \quad y := x' - y' * \left\lfloor \frac{n}{m} \right\rfloor$
34	0	34	1	0	$\texttt{if}\ (m = 0)\ \texttt{return}\ (n, 1, 0)$

Table: Test run of the extended Euclidean Algorithm

Extended Euclidian Algorithm

Example: What is the greatest common divisor of $n = 170$ and $m = 102$?

n	m	g	x	y	Remark
170	102	34	-1	2	
102	68	34	1	-1	
68	34	34	0	1	$x := y'; \quad y := x' - y' * \left\lfloor \frac{n}{m} \right\rfloor$
34	0	34	1	0	if $(m = 0)$ return $(n, 1, 0)$

Table: Test run of the extended Euclidean Algorithm

Extended Euclidian Algorithm

Example: What is the greatest common divisor of $n = 170$ and $m = 102$?

n	m	g	x	y	Remark
170	102	34	-1	2	
102	68	34	1	-1	
68	34	34	0	1	$x := y'; \quad y := x' - y' * \left\lfloor \frac{n}{m} \right\rfloor$
34	0	34	1	0	$\texttt{if } (m = 0) \texttt{ return } (n, 1, 0)$

Table: Test run of the extended Euclidean Algorithm

This result indeed is correct, since

$$(\mathbf{-1}) \cdot 170 + \mathbf{2} \cdot 102 = \mathbf{34} = \texttt{gcd}(170, 102).$$

Algebra and Number Theory: Group, Ring, and Field

Definition

- A *group* $\mathfrak{G} = (S, \circ)$ is defined by a nonempty set S and a binary operation $\circ$ on S satisfying the following axioms:
  - **Closure:** $(\forall x \in S)\,(\forall y \in S)\,[x \circ y \in S]$.
  - **Associativity:** $(\forall x \in S)\,(\forall y \in S)\,(\forall z \in S)\,[(x \circ y) \circ z = x \circ (y \circ z)]$.
  - **Neutral element:** $(\exists e \in S)\,(\forall x \in S)\,[e \circ x = x \circ e = x]$.
  - **Inverse element:** $(\forall x \in S)\,(\exists x^{-1} \in S)\,[x \circ x^{-1} = x^{-1} \circ x = e]$.
- The element e is called the *neutral element of the group $\mathfrak{G}$*.
- The element x^{-1} is called the *inverse element of x*.
- Define the *order of an element x of $\mathfrak{G}$* to be the smallest positive integer k such that $x^k = \underbrace{x \circ x \circ \cdots \circ x}_{k \text{ times}} = e$.

Algebra and Number Theory: Group, Ring, and Field

Definition

- $\mathfrak{M} = (S, \circ)$ is a *semi-group* if it satisfies associativity and closure under $\circ$. A semi-group $\mathfrak{M}$ might have no neutral element (if it does, it is a *monoid*), and not every element in $\mathfrak{M}$ might have an inverse.

- A group $\mathfrak{G} = (S, \circ)$ (respectively, a semi-group or monoid $\mathfrak{M} = (S, \circ)$) is said to be *commutative* (or *abelian*) if and only if for each $x, y \in S$,
  $$x \circ y = y \circ x.$$
  The number of elements of a finite group $\mathfrak{G}$ is said to be the *order of $\mathfrak{G}$* and is denoted by $\|\mathfrak{G}\|$.

- $\mathfrak{H} = (T, \circ)$ is said to be a *subgroup of $\mathfrak{G} = (S, \circ)$* (denoted by $\mathfrak{H} \leq \mathfrak{G}$) if and only if $T \subseteq S$ and $\mathfrak{H}$ satisfies the group axioms.

Algebra and Number Theory: Group, Ring, and Field

Definition

- A *ring* is a triple $\mathfrak{R} = (S, +, \cdot)$ such that
  - $(S, +)$ is an abelian group,
  - $(S, \cdot)$ is a semi-group, and
  - the distributive laws are satisfied for all x, y, and z in S:

$$\begin{aligned} x \cdot (y + z) &= (x \cdot y) + (x \cdot z); \\ (x + y) \cdot z &= (x \cdot z) + (y \cdot z). \end{aligned}$$

- A ring $\mathfrak{R} = (S, +, \cdot)$ is said to be *commutative* if and only if the semi-group $(S, \cdot)$ is commutative.

Algebra and Number Theory: Group, Ring, and Field

Definition

- Let $\mathfrak{R} = (S, +, \cdot)$ be a ring.
  - The neutral element of the group $(S, +)$ is said to be the *zero element* (the *zero*, for short) of $\mathfrak{R}$.
  - The neutral element of the semi-group $(S, \cdot)$, if it exists, is said to be the *one element* (the *one*, for short) of $\mathfrak{R}$.
- Let $\mathfrak{R} = (S, +, \cdot)$ be a ring with one. An element x of $\mathfrak{R}$ is *invertible* if and only if it is invertible in the monoid $(S, \cdot)$.
- A *field* is a commutative ring with one in which each element distinct from zero is invertible.

Algebra and Number Theory: Group, Ring, and Field

Example:

- Let $k \in \mathbb{N}_+$.
  - The set $\mathbb{Z}_k = \{0, 1, \ldots, k-1\}$ is a finite group with respect to addition modulo k, and with the neutral element 0.
  - With respect to addition and multiplication modulo k, $\mathbb{Z}_k$ is a commutative ring with one.
  - If p is a *prime number* (i.e., $p \geq 2$ is divisible by 1 and by p only), then $\mathbb{Z}_p$ is a field with respect to addition and multiplication modulo p.

- For any fixed $k \in \mathbb{N}_+$, define the set

$$\mathbb{Z}_k^* = \{i \,\big|\, 1 \leq i \leq k-1 \text{ and } \mathtt{gcd}(i,k) = 1\}.$$

With respect to multiplication modulo k, $\mathbb{Z}_k^*$ is a finite group with the neutral element 1.

Algebra and Number Theory: Group, Ring, and Field

- How do we find the inverse of i in $\mathbb{Z}_k^*$?
- With the extended Euclidean Algorithm!
- Recall from our example: $(\mathbf{-1}) \cdot 170 + \mathbf{2} \cdot 102 = \mathbf{34} = \mathtt{gcd}(170, 102)$.
- However, if we have $\mathtt{gcd}(n, m) = \mathbf{1} = \mathbf{x} \cdot n + \mathbf{y} \cdot m$, then in the arithmetics modulo n:

  $$\mathbf{y} \cdot m \equiv \mathbf{1} \bmod n,$$

  so $\mathbf{y} = m^{-1}$.
- For example, with the extended Euclidean Algorithm we get:

  $$\mathtt{gcd}(26, 11) = \mathbf{1} = \mathbf{3} \cdot 26 + (\mathbf{-7}) \cdot 11 = 78 - 77, \text{ so}$$
  $$11^{-1} = (\mathbf{-7}) \equiv 19 \bmod 26.$$

Back to the Affine Cipher

Let $M = C = \mathbb{Z}_{26}$ and $K = \{(a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} \,|\, \mathtt{gcd}(a,26) = 1\}$.

For each key $(a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$ with $\mathtt{gcd}(a,26) = 1$, the encryption function $E_{(a,b)}$ and the decryption function $D_{(a^{-1},b)}$, which both map from $\mathbb{Z}_{26}$ to $\mathbb{Z}_{26}$, are defined by:

$$\begin{aligned} E_{(a,b)}(x) &= ax + b \bmod 26; \\ D_{(a^{-1},b)}(y) &= a^{-1}(y-b) \bmod 26, \end{aligned}$$

where a^{-1} is the inverse element of a in $\mathbb{Z}_{26}$, i.e., $aa^{-1} \equiv a^{-1}a \equiv 1 \bmod 26$. Note that a^{-1} can easily be determined by the *extended algorithm of Euclid*.

Back to the Affine Cipher

Example:

- Choose the encryption key $k = (5, 7)$.
- Note that 21 is the inverse element of 5 modulo 26, since

$$5 \cdot 21 = 105 = 1 + 4 \cdot 26 \equiv 1 \bmod 26.$$

- Hence, the decryption key is $k' = (21, 7)$.
- Consider the message m and determine its encryption c:

m	T H E E L E C T I V E A F F I N I T I E S B Y G O E T H E
c	

Table: Example of an encryption by the affine cipher with key $k = (5, 7)$

Back to the Affine Cipher

- The first plaintext letter is a "T," which is encoded as 19.
- The corresponding first letter of the ciphertext is determined by

$$E_{(5,7)}(19) = 5 \cdot 19 + 7 \equiv 24 \bmod 26.$$

  Thus the ciphertext letter "Y," which corresponds to 24, encrypts "T."
- With decryption key $k' = (21, 7)$ we can correctly decipher this letter:

$$D_{(21,7)}(24) = 21(24 - 7) = 357 \equiv 19 \bmod 26.$$

- Overall, we obtain:

m	T H E E L E C T I V E A F F I N I T I E S B Y G O E T H E
c	Y Q B B K B R Y V I B H G G V U V Y V B T M X L Z B Y Q B

Table: Example of an encryption by the affine cipher with key $k = (5, 7)$

Back to the Affine Cipher

In general, if y is a ciphertext letter encrypting a plaintext letter x with key (a, b), we have

$$\begin{aligned} y \equiv ax + b \bmod 26 \quad &\iff \quad ax \equiv y - b \bmod 26 \\ &\iff \quad a^{-1}ax \equiv a^{-1}(y - b) \bmod 26 \\ &\iff \quad x \equiv a^{-1}(y - b) \bmod 26, \end{aligned}$$

which shows that the affine cipher indeed is a cryptosystem.

Cryptanalysis of the Affine Cipher

Observation:

- For the alphabet $\mathbb{Z}_{26}$, the affine cipher has only

  $$26 \cdot \varphi(26) = 26 \cdot 12 = 312$$

  keys, since

  - the number of choices for $b \in \mathbb{Z}_{26}$ is 26 and
  - the number of choices for $a \in \mathbb{Z}_{26}$ coprime with 26 is $\varphi(26) = 12$,

  where $\varphi(k) = \|\mathbb{Z}_k^*\|$ is the *Euler function*.

  Thus, a *ciphertext-only attack* breaks the affine cipher by brute force, i.e., by an exhaustive search of the key space.

- The affine cipher can also be broken by a *known-plaintext attack* in which two plaintext letters and their encryptions are known.

Cryptanalysis of the Affine Cipher

Example (Known-Plaintext Attack Against the Affine Cipher)

Suppose that the cryptanalyst knows the ciphertext c from our previous example, and he also knows the first two plaintext symbols, "T" and "H," corresponding to the first two ciphertext letters, "Y" and "Q."

He can then determine the keys as follows:

- Since "Y" encrypts "T" and "Q" encrypts "H," one obtains the congruences:

$$\begin{aligned} 19a + b &\equiv 24 \bmod 26; && (1) \\ 7a + b &\equiv 16 \bmod 26; && (2) \end{aligned}$$

Cryptanalysis of the Affine Cipher

- (2) is equivalent to $b \equiv 16 - 7a \bmod 26$.
- Substituting this into (1) gives $19a + 16 - 7a \equiv 24 \bmod 26$ and thus $12a \equiv 8 \bmod 26$, which implies
$$6a \quad \equiv \quad 4 \bmod 13. \tag{3}$$
Why? Because we can cancel modulo m as follows:
$$c \cdot e \equiv c \cdot f \bmod m \iff e \equiv f \bmod \frac{m}{\gcd(c,m)}.$$
- Multiplying (3) with the inverse element 11 of 6 modulo 13 yields
$$a \quad \equiv \quad 44 \equiv 5 \bmod 13.$$
- It follows that $a = 5$ and $b = 7$.

Solving Congruences modulo m

$$c \cdot a \equiv d \bmod m \tag{4}$$

is solvable in a if and only if $g = \mathtt{gcd}(c, m)$ divides d.

The number of solutions $\bmod m$ of (4) then is g and all solutions are congruent to each other $\bmod {}^{m}\!/_{g}$:

$$g = x \cdot c + y \cdot m \qquad \text{by the extended Euclidian Algorithm}$$

gives the following solutions for (4):

$$a_1 = \frac{x \cdot d}{g} \quad \text{and} \quad a_i = a_1 + (i-1)\frac{m}{g} \quad \text{for } i = 2, \ldots, g.$$

The Method of Frequency Counts

The method of *frequency counts* is often useful for breaking monoalphabetic cryptosystems (e.g., the shift cipher and the affine cipher). It exploits the *redundancy* of the natural language used for encryption.

Letters occurring with high frequency										Total
Letter	E	T	A	O	N	I	S	R	H	
Frequency in %	12.31	9.59	8.05	7.94	7.19	7.18	6.59	6.03	5.14	**70.02%**

Letters occurring with medium frequency										
Letter	L	D	C	U	P	F	M	W	Y	
Frequency in %	4.03	3.65	3.20	3.10	2.29	2.28	2.25	2.03	1.88	**24.71%**

Letters occurring with low frequency										
Letter	B	G	V	K	Q	X	J	Z		
Frequency in %	1.62	1.61	0.93	0.52	0.20	0.20	0.10	0.09		**5.27%**

Cryptanalysis of the Affine Cipher by Frequency Counts

In our previous example:

c	Y Q B B K B R Y V I B H G G V U V Y V B T M X L Z B Y Q B

we have:

Letter	B	Y	V	Q	G	K	R	I	H	U	T	M	X	L	Z
Frequency	7	4	4	2	2	1	1	1	1	1	1	1	1	1	1

Table: Frequencies of letters in the ciphertext from the above example

$\Longrightarrow$ Erich guesses that "B" encrypts "E," and that "Y" and "V" each encrypt one of the letters "T," "A," "O," "N," or "I."

Cryptanalysis of the Affine Cipher by Frequency Counts

c	Y Q B B K B R Y V I B H G G V U V Y V B T M X L Z B Y Q B
V is A	T H E E ? E ? T A ? E ? ? ? A ? A T A E ? ? ? ? ? E T H E
V is O	T H E E ? E ? T O ? E ? ? ? O ? O T O E ? ? ? ? ? E T H E
V is N	T H E E ? E ? T N ? E ? ? ? N ? N T N E ? ? ? ? ? E T H E
V is I	T H E E ? E ? T I ? E ? ? ? I ? I T I E ? ? ? ? ? E T H E

Table: Guessing in the frequency counts method: B is E, Y is T, Q is H

Cryptanalysis of the Affine Cipher by Frequency Counts

c	YQB BKBRYVIB HGGVUVYVBT MX LZBYQB
V is A	THE E?E?TA?E ???A?ATAE? ?? ??ETHE
V is O	THE E?E?TO?E ???O?OTOE? ?? ??ETHE
V is N	THE E?E?TN?E ???N?NTNE? ?? ??ETHE
V is I	THE E?E?TI?E ???I?ITIE? ?? ??ETHE

Table: Guessing in the frequency counts method: B is E, Y is T, Q is H

Cryptanalysis of the Affine Cipher by Frequency Counts

c	YQB BKBRYVIB HGGVUVYVBT MX LZBYQB

V is A	THE E?E?TA?E ???A?ATAE? ?? ??ETHE
V is O	THE E?E?TO?E ???O?OTOE? ?? ??ETHE
V is N	THE E?E?TN?E ???N?NTNE? ?? ??ETHE
V is I	THE E?E?TI?E ???I?ITIE? ?? ??ETHE

⋮

m	THE ELECTIVE AFFINITIES BY GOETHE

Table: Guessing in the frequency counts method: B is E, Y is T, Q is H

Cryptanalysis of the Affine Cipher by Frequency Counts

Example (Stinson (2002))

c	F M X V E D K A P H F E R B N D K R X R S R E F M O R U D S D K D V S H V U F E D K A P R K D L Y E V L R H H R H

Now we have:

Letter	R	D	E	H	K	F	V	S	A	L	M	P	U	X	B	N	O	Y
Frequency	8	7	5	5	5	4	4	3	2	2	2	2	2	2	1	1	1	1

Table: Frequencies of letters in the ciphertext from the above example

Our goal is to determine the key (a, b) used in the encryption by the affine cipher:

$$E_{(a,b)}(x) = ax + b \bmod 26.$$

Cryptanalysis of the Affine Cipher by Frequency Counts

Example (Stinson (2002) continued)

- **Hypothesis 1: R encrypts E and D encrypts T.**

  Thus $E_{(a,b)}(4) = 17$ and $E_{(a,b)}(19) = 3$.

  This gives a system of equations with two unknowns:

$$\begin{aligned} 4a + b &= 17 \\ 19a + b &= 3 \end{aligned}$$

  Subtracting the first from the second equation modulo 26 gives:

$$15a = 12,$$

  and since $15^{-1} = 7 \bmod 26$, we have the solution

$$a = 7 \cdot 12 = 84 \equiv 6 \bmod 26 \quad \text{and} \quad b = 19 \quad \text{in} \quad \mathbb{Z}_{26}.$$

  However, $(6, 19)$ is not an allowed key because $\gcd(6, 26) = 2 > 1$.

Cryptanalysis of the Affine Cipher by Frequency Counts

Example (Stinson (2002) continued)

- **Hypothesis 2: R encrypts E and E encrypts T.**

  Thus $E_{(a,b)}(4) = 17$ and $E_{(a,b)}(19) = 4$.

  This gives a system of equations with two unknowns:

$$\begin{aligned} 4a + b &= 17 \\ 19a + b &= 4 \end{aligned}$$

  Subtracting the first from the second equation modulo 26 gives:

$$15a = 13,$$

  and since $15^{-1} = 7 \bmod 26$, we have the solution

$$a = 7 \cdot 13 = 91 \equiv 13 \bmod 26 \quad \text{and} \quad b = 17 \quad \text{in} \quad \mathbb{Z}_{26}.$$

  However, $(13, 17)$ is not an allowed key because $\gcd(13, 26) = 13 > 1$.

Cryptanalysis of the Affine Cipher by Frequency Counts

Example (Stinson (2002) continued)

- **Hypothesis 3: R encrypts E and H encrypts T.**

  Then $a = 8$. However, $\mathtt{gcd}(8, 26) = 2 > 1$.

- **Hypothesis 4: R encrypts E and K encrypts T.**

  Then $a = 3$ and $b = 5$. **BINGO!** $(3, 5)$ **is the key used:**

  To verify, determine $a^{-1} = 3^{-1} = 9 \bmod 26$, so

  $$a^{-1} \cdot b = 9 \cdot 5 = 45 \equiv 19 \bmod 26.$$

  Now decrypt the ciphertext with the decryption function

  $$D_{(a^{-1},b)}(y) = a^{-1}(y - b) = 9 \cdot y - 19 \bmod 26:$$

m	ALGORITHMSAREQUITEGENERALDEFI
	NITIONSOFARITHMETICPROCESSES

Cryptanalysis of a Substitution Cipher by Frequency Counts

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

Table: Example due to Stinson (2002)

Cryptanalysis of a Substitution Cipher by Frequency Counts

Example (Stinson (2002))

- Z occurs 20 times, more often than any other letter, so we guess that Z encrypts the plaintext letter e. (NOTE: In this example, plaintext letters are lower-case and ciphertext letters are UPPER-case.)
- C, D, F, J, M, R, Y occur at least 10 times each, so we guess that they encrypt (a subset of) t, a, o, i, n, s, h, r.
  It is unclear, though, which encrypts which letter.
- Let's have a look at **digrams**, especially those containing Z:
  - DZ and ZW occur 4 times each;
  - NZ and ZU occur 3 times each;
  - RZ, HZ, XZ, FZ and ZR, ZV, ZC, ZD, ZJ occur 2 times each.

Cryptanalysis of a Substitution Cipher by Frequency Counts

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

Table: Looking for digrams containing Z

Cryptanalysis of a Substitution Cipher by Frequency Counts

Example (Stinson (2002) continued)

- Since ZW occurs 4 times and WZ occurs not at all, we guess that W encrypts d.
- Since DZ occurs 4 times and ZD twice, we guess that D encrypts one of r, s, t. It is unclear, though, which letter exactly.
- Under our assumption that Z encrypts e and W encrypts d, we look at **trigrams**, especially those containing Z and W:
  - ZRW and RZW occur in the first line;
- Later, we also have RW. Since nd is a frequently used digram in English, we guess that R encrypts n.

Cryptanalysis of a Substitution Cipher by Frequency Counts

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

Table: Looking for trigrams containing Z and W and the digram RW

Cryptanalysis of a Substitution Cipher by Frequency Counts

						e	n	d										e					n	e	d		
Y	I	F	Q	F	M	Z	R	W	Q	F	Y	V	E	C	F	M	D	Z	P	C	V	M	R	Z	W	N	M
	e																					e					e
D	Z	V	E	J	B	T	X	C	D	D	U	M	J	N	D	I	F	E	F	M	D	Z	C	D	M	Q	Z
									n			d				e	n					e					e
K	C	E	Y	F	C	J	M	Y	R	N	C	W	J	C	S	Z	R	E	X	C	H	Z	U	N	M	X	Z
	e				n							n							e	d				e			
N	Z	U	C	D	R	J	X	Y	Y	S	M	R	T	M	E	Y	I	F	Z	W	D	Y	V	Z	V	Y	F
e			n	e		n	d		e		e				e	d						n					
Z	U	M	R	Z	C	R	W	N	Z	D	Z	J	J	X	Z	W	G	C	H	S	M	R	N	M	D	H	N
						e					e	d								d				e			n
C	M	F	Q	C	H	Z	J	M	X	J	Z	W	I	E	J	Y	U	C	F	W	D	J	N	Z	D	I	R

Table: Guessing: Z encrypts e, W encrypts d, and R encrypts n

Cryptanalysis of a Substitution Cipher by Frequency Counts

Example (Stinson (2002) continued)

- Since NZ occurs 3 times and ZN only once and since he occurs more often than eh in typical English texts, we guess that N encrypts h.
- Now, the string n e – n d h e in the (guessed) plaintext suggests that C encrypts a.

Cryptanalysis of a Substitution Cipher by Frequency Counts

						e	n	d						a				e		a			n	e	d	h	
Y	I	F	Q	F	M	Z	R	W	Q	F	Y	V	E	C	F	M	D	Z	P	C	V	M	R	Z	W	N	M
	e							a						h								e	a				e
D	Z	V	E	J	B	T	X	C	D	D	U	M	J	N	D	I	F	E	F	M	D	Z	C	D	M	Q	Z
	a				a				n	h	a	d		a		e	n			a		e		h			e
K	C	E	Y	F	C	J	M	Y	R	N	C	W	J	C	S	Z	R	E	X	C	H	Z	U	N	M	X	Z
h	e		a		n							n							e	d				e			
N	Z	U	C	D	R	J	X	Y	Y	S	M	R	T	M	E	Y	I	F	Z	W	D	Y	V	Z	V	Y	F
e			n	e	a	n	d	h	e		e				e	d		a				n	h				h
Z	U	M	R	Z	C	R	W	N	Z	D	Z	J	J	X	Z	W	G	C	H	S	M	R	N	M	D	H	N
a				a		e					e	d						a		d			h	e			n
C	M	F	Q	C	H	Z	J	M	X	J	Z	W	I	E	J	Y	U	C	F	W	D	J	N	Z	D	I	R

Table: Guessing: Z is e, W is d, R is n, N is h, and C is a

Cryptanalysis of a Substitution Cipher by Frequency Counts

Example (Stinson (2002) continued)

- Consider M, the letter occurring with the second-most frequency in the ciphertext (after Z).
- RNM (which we guess encrypts n h ?) suggests that h starts a new word.
- Thus M very likely encrypts a vowel. Since
  - e and a are (very likely) gone and
  - u is rare but M occurs 16 times,

  it is very likely that M encrypts either i or o.
- ai is more likely than ao.

  Thus CM (last line, left) suggests that M encrypts i.

Cryptanalysis of a Substitution Cipher by Frequency Counts

					i	e	n	d						a		i		e		a		i	n	e	d	h	i
Y	I	F	Q	F	M	Z	R	W	Q	F	Y	V	E	C	F	M	D	Z	P	C	V	M	R	Z	W	N	M
	e							a				i		h						i		e	a		i		e
D	Z	V	E	J	B	T	X	C	D	D	U	M	J	N	D	I	F	E	F	M	D	Z	C	D	M	Q	Z
	a				a		i		n	h	a	d		a		e	n			a		e		h	i		e
K	C	E	Y	F	C	J	M	Y	R	N	C	W	J	C	S	Z	R	E	X	C	H	Z	U	N	M	X	Z
h	e		a		n						i	n		i					e	d				e			
N	Z	U	C	D	R	J	X	Y	Y	S	M	R	T	M	E	Y	I	F	Z	W	D	Y	V	Z	V	Y	F
e		i	n	e	a	n	d	h	e		e				e	d		a			i	n	h	i			h
Z	U	M	R	Z	C	R	W	N	Z	D	Z	J	J	X	Z	W	G	C	H	S	M	R	N	M	D	H	N
a	i			a		e		i			e	d						a		d			h	e			n
C	M	F	Q	C	H	Z	J	M	X	J	Z	W	I	E	J	Y	U	C	F	W	D	J	N	Z	D	I	R

Table: Guessing: Z is e, W is d, R is n, N is h, C is a, and M is i

Cryptanalysis of a Substitution Cipher by Frequency Counts

Example (Stinson (2002) continued)

- Which letter encrypts o?
- Since o is a frequent letter, we suspect D, F, J, Y—each are similarly frequent in English.
- Among those, Y is most likely to encrypt o, for otherwise we would have "vowel worms" like aoi because of CFM and CJM.
- We now suspect D, F, J to each encrypt one of r, s, t:
  - NMD (i.e., h i ?) occurs twice, suggesting that D encrypts s.
  - Also, HNCMF (i.e., ? h a i ?) looks like c h a i r, so H is likely to encrypt c and F to encrypt r.
  - Thus J very likely encrypts t.

Cryptanalysis of a Substitution Cipher by Frequency Counts

o	u	r	f	r	i	e	n	d	f	r	o	m	p	a	r	i	s	e	x	a	m	i	n	e	d	h	i
Y	I	F	Q	F	M	Z	R	W	Q	F	Y	V	E	C	F	M	D	Z	P	C	V	M	R	Z	W	N	M
s	e	m	p	t	y	g	l	a	s	s	w	i	t	h	s	u	r	p	r	i	s	e	a	s	i	f	e
D	Z	V	E	J	B	T	X	C	D	D	U	M	J	N	D	I	F	E	F	M	D	Z	C	D	M	Q	Z
v	a	p	o	r	a	t	i	o	n	h	a	d	t	a	k	e	n	p	l	a	c	e	w	h	i	l	e
K	C	E	Y	F	C	J	M	Y	R	N	C	W	J	C	S	Z	R	E	X	C	H	Z	U	N	M	X	Z
h	e	w	a	s	n	t	l	o	o	k	i	n	g	i	p	o	u	r	e	d	s	o	m	e	m	o	r
N	Z	U	C	D	R	J	X	Y	Y	S	M	R	T	M	E	Y	I	F	Z	W	D	Y	V	Z	V	Y	F
e	w	i	n	e	a	n	d	h	e	s	e	t	t	l	e	d	b	a	c	k	i	n	h	i	s	c	h
Z	U	M	R	Z	C	R	W	N	Z	D	Z	J	J	X	Z	W	G	C	H	S	M	R	N	M	D	H	N
a	i	r	f	a	c	e	t	i	l	t	e	d	u	p	t	o	w	a	r	d	s	t	h	e	s	u	n
C	M	F	Q	C	H	Z	J	M	X	J	Z	W	I	E	J	Y	U	C	F	W	D	J	N	Z	D	I	R

Table: Example due to Stinson (2002)

Cryptanalysis of a Substitution Cipher by Frequency Counts

Our friend from Paris examined his empty glass with surprise, as if evaporation had taken place while he wasn't looking. I poured some more wine and he settled back in his chair, face tilted up towards the sun.

P. Mayle, *A Year in Provence*, A. Knopf, Inc., 1989

Vigenère Cipher

This symmetric polyalphabetic cryptosystem uses a *Vigenère square*:

0	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
1	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	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

Vigenère Cipher

- Messages are subdivided into blocks of length n, and are then encrypted block-wise. That is, $K = M = C = \mathbb{Z}_{26}^n$, where n is the block length of the system.
- For each key $\vec{k} \in \mathbb{Z}_{26}^n$, the encryption function $E_{\vec{k}}$ and the decryption function $D_{\vec{k}}$, both mapping from $\mathbb{Z}_{26}^n$ to $\mathbb{Z}_{26}^n$, are defined by:

$$\begin{array}{rcl} E_{\vec{k}}(\vec{x}) & = & (\vec{x} + \vec{k}) \bmod 26 \\ D_{\vec{k}}(\vec{y}) & = & (\vec{y} - \vec{k}) \bmod 26, \end{array}$$

  where addition and subtraction with $\vec{k}$ modulo 26 are carried out character-wise.

Vigenère Cipher

- More concretely, the key $\vec{k} \in \mathbb{Z}_{26}^n$ is written symbol by symbol above each block $\vec{x} \in \mathbb{Z}_{26}^n$ of the plaintext. If the last block has less than n symbols, use less symbols of the key accordingly.

- Let s_i denote the i^{th} symbol of any given string $\vec{s}$.

- To encrypt the i^{th} plaintext symbol x_i, with the i^{th} key symbol k_i sitting on top of it, use the i^{th} row of the Vigenère square as if it were the shift cipher with key k_i.

- Observe that one and the same plaintext symbol can thus be encrypted by distinct ciphertext symbols.

Vigenère Cipher

- For example, choose the period $n = 4$ and the key $\vec{k} = \mathrm{ELLA}$.
  The table:

key	E L L A E L L A E L L A E L L A E L L A E L L A E L L A
message	H U N G A R I A N I S A L L G R E E K T O G E R M A N S
ciphertext	L F Y G E C T A R T D A P W R R I P V T S R P R Q L Y S

Table: Example of an encryption by the Vigenère cipher with key ELLA

shows the encryption of a plaintext consisting of seven blocks into a ciphertext using the Vigenère cipher with this key.

- The first letter of the plaintext, "H," has the key symbol "E" above it.
- The "H"-column intersects with the "E"-row of the Vigenère square at "L," which is thus the first symbol of the ciphertext.

Vigenère Cipher

- Distinct ciphertext symbols encrypt the same plaintext symbol:
  - the plaintext letter "A" occurs four times and is encrypted by "A" twice, by "E" once, and by "L" once;
  - the plaintext letter "E" occurs three times and is encrypted by "I" once and by "P" twice;
  - the plaintext letter "G" occurs three times and is encrypted by "G" once and by "R" twice;
  - the plaintext letter "N" occurs three times and is encrypted by "R" once and by "Y" twice;
  - the plaintext letter "R" occurs three times and is encrypted by "C" once and by "R" twice.
- This observation also shows two weaknesses of the key chosen:
  - two letters of the key ELLA are equal, and
  - one letter of the key is "A," which does not alter the corresponding cleartext letters.

Affine Linear Block Ciphers

- The Vigenère cipher is a special case of an *affine linear block cipher*, which generalizes the affine cipher.
- Before defining affine linear block ciphers, we recall some elementary notions from linear algebra.
- In particular, affine linear block ciphers require operations on matrices over the ring $\mathbb{Z}_m$, i.e.,
  - the matrix entries are elements of $\mathbb{Z}_m$ and
  - the matrix operations are based on the arithmetics modulo m.

Inverse Matrix, Determinant, and Adjoint Matrix

Definition

- Let $\vec{u}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ denote the i^{th} *unity vector of length n*:
  - the i^{th} coordinate of $\vec{u}_i$ is one, and
  - the j^{th} coordinate of $\vec{u}_i$ is zero for all $j \neq i$.
- The *$(n \times n)$ unity matrix* is defined by $U_n = (\vec{u}_i)_{1 \leq i \leq n}$, where the i^{th} row (and column) of U_n is the i^{th} unity vector of length n.
- Consider an $(n \times n)$ matrix A over the ring $\mathbb{Z}_m$. The *(multiplicative) inverse of A*, denoted by A^{-1}, is an $(n \times n)$ matrix satisfying that
$$AA^{-1} = A^{-1}A$$
is the $(n \times n)$ unity matrix U_n.

Inverse Matrix, Determinant, and Adjoint Matrix

Definition

- The *determinant of A* can be defined recursively:
  - for $n = 1$ and $A = (a)$, $\det A = a$;
  - for $n > 1$ and for each $i \in \{1, 2, \ldots, n\}$,

    $$\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{i,j} \det A_{i,j},$$

    where $a_{i,j}$ is the (i,j)-entry of A, and the $((n-1) \times (n-1))$ matrix $A_{i,j}$ results from A by canceling out the i^{th} row and the j^{th} column.

- Define the *adjoint matrix of A* by $A_{\mathtt{adj}} = ((-1)^{i+j} \det A_{j,i})$.

Inverse Matrix, Determinant, and Adjoint Matrix

Remark:

- $\mathbb{Z}_m^{n \times n}$ is a ring with one (in general, not commutative) with respect to
  - addition: $A + B = (a_{i,j} + b_{i,j} \bmod m)$ for $A = (a_{i,j}), B = (b_{i,j}) \in \mathbb{Z}_m^{n \times n}$, and
  - multiplication: $A \cdot B = (c_{i,j})$ with $c_{i,j} = \sum_{k=1}^{n} a_{i,k} \cdot b_{k,j} \bmod m$
- An $(n \times n)$ matrix A over the ring $\mathbb{Z}_m$ has a multiplicative inverse matrix if and only if $\mathtt{gcd}(\det A, m) = 1$.
- In general, an $(n \times n)$ matrix over the reals is invertible if and only if its determinant is nonzero.
- The determinant of a matrix can be computed efficiently.
- It can be shown that $A^{-1} = (\det A)^{-1} A_{\mathtt{adj}}$.

Inverse Matrix, Determinant, and Adjoint Matrix

Example

Let $m = 7$ and $A = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$ and $B = \begin{pmatrix} 4 & 5 \\ 6 & 0 \end{pmatrix}$. Then

$$A + B = \begin{pmatrix} 5 & 0 \\ 1 & 3 \end{pmatrix} \text{ and } A \cdot B = \begin{pmatrix} 4+12 \bmod 7 & 5+0 \bmod 7 \\ 8+18 \bmod 7 & 10+0 \bmod 7 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ 5 & 3 \end{pmatrix}.$$

Since $B \cdot A = \begin{pmatrix} 0 & 2 \\ 6 & 5 \end{pmatrix}$, we see that multiplication is not commutative.

We write $A \equiv B \bmod m$ if $a_{i,j} \equiv b_{i,j} \bmod m$ for $1 \leq i, j \leq m$.

Inverse Matrix, Determinant, and Adjoint Matrix

Example

For $A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$, we have

$$A_{1,1} = (a_{2,2}), \quad A_{1,2} = (a_{2,1}), \quad A_{2,1} = (a_{1,2}), \quad A_{2,2} = (a_{1,1}).$$

Thus

$$\det A = a_{1,1} \cdot a_{2,2} - a_{1,2} \cdot a_{2,1}$$

and

$$A_{\mathtt{adj}} = \begin{pmatrix} a_{2,2} & -a_{1,2} \\ -a_{2,1} & a_{1,1} \end{pmatrix}.$$

Inverse Matrix, Determinant, and Adjoint Matrix

Example

Let $m = 11$. We want to determine the inverse of $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, i.e., we want to solve the congruence

$$A \cdot A^{-1} \equiv U_2 \bmod 11.$$

This solution (and A^{-1}) exists if and only if $\texttt{gcd}(\det A, 11) = 1$.

Since $\det A = 4 - 6 = -2$, we indeed have $\texttt{gcd}(\det A, 11) = \texttt{gcd}(9, 11) = 1$.

Moreover, $(-2)(-6) = 12 \equiv 1 \bmod 11$, so

$$(\det A)^{-1} = 9^{-1} = -6 \equiv 5 \bmod 11.$$

Inverse Matrix, Determinant, and Adjoint Matrix

Example (continued)

It follows that

$$\begin{aligned} A^{-1} &= (\det A)^{-1} A_{\mathtt{adj}} \bmod 11 \\ &= 5 \cdot \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} \bmod 11 = \begin{pmatrix} 9 & 1 \\ 7 & 5 \end{pmatrix}. \end{aligned}$$

This is indeed correct because

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 9 & 1 \\ 7 & 5 \end{pmatrix} \bmod 11 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Affine Linear Block Ciphers

Definition

A block cipher with plaintext and ciphertext space $\mathbb{Z}_m^n$ and block length n is said to be *affine linear* if and only if all its encryption functions are affine linear. That is, they all are of the following form:

$$E_{(A,\vec{b})}(\vec{x}) \;=\; A\vec{x}+\vec{b} \bmod m, \tag{5}$$

where A is an $(n \times n)$ matrix with entries from $\mathbb{Z}_m$ such that $\gcd(\det A, m) = 1$, and $\vec{x}$, $\vec{y}$, and $\vec{b}$ are vectors in $\mathbb{Z}_m^n$; all arithmetics is done modulo m. The corresponding decryption function is

$$D_{(A^{-1},\vec{b})}(\vec{y}) \;=\; A^{-1}(\vec{y}-\vec{b}) \bmod m,$$

where A^{-1} is the inverse matrix for A.

Linear and Affine Linear Block Ciphers

Definition

A *linear block cipher* is an affine linear block cipher for which $\vec{b}$ in (5) is the zero vector.

Example

- The Vigenère cipher is affine linear.
- A classical example of a linear cipher is the *Hill cipher*, invented by Lester Hill in 1929:

  In fact, the Hill cipher is the most general linear block cipher.

Hill Cipher

- Let Σ be an alphabet with m letters, and let n be the block length.
- The plaintext and cipher text space is $M = C = \mathbb{Z}_m^n$.
- The key space K is the set of all $(n \times n)$ matrices A with entries from $\mathbb{Z}_m$ such that $\mathtt{gcd}(\det A, m) = 1$. This condition ensures that the matrices are invertible, since the inverse matrix A^{-1} is used as the decryption key corresponding to the encryption key A.
- The encryption function E_A and the decryption function $D_{A^{-1}}$ are defined by:

$$\begin{aligned} E_A(\vec{x}) &= A\vec{x} \bmod m; \\ D_{A^{-1}}(\vec{y}) &= A^{-1}\vec{y} \bmod m. \end{aligned}$$

Hill Cipher

The Hill cipher works best if the size m of the alphabet is a prime number.

To achieve this, one usually adds to the 26 letters of the English alphabet:

- the blank $\square$ (encoded as 26),
- the comma (encoded as 27), and
- the full stop (encoded as 28)

Thus, $m = 29$ is a prime number and all arithmetics is done over $\mathbb{Z}_{29}$.

Hill Cipher

Example

- Choose the block length $n = 2$ and
- an invertible (2×2) matrix A, and
- compute the inverse matrix A^{-1} in the arithmetics modulo 29.

For example, choose

$$A = \begin{pmatrix} 3 & 4 \\ 7 & 2 \end{pmatrix}$$

$$\Longrightarrow \qquad \det A = 3 \cdot 2 - 4 \cdot 7 = -22 \equiv 7 \bmod 29$$

and, using the extended Euclidean algorithm, we obtain

$$1 \cdot 29 - 4 \cdot 7 \equiv 1 \bmod 29, \qquad \text{so} \qquad (\det A)^{-1} = 7^{-1} = -4 \equiv 25 \bmod 29.$$

Hill Cipher

Example (continued)

$$\begin{aligned} A^{-1} &\equiv (\det A)^{-1} A_{\mathtt{adj}} \bmod 29 \equiv 25 \cdot \begin{pmatrix} 2 & -4 \\ -7 & 3 \end{pmatrix} \bmod 29 \\ &\equiv \begin{pmatrix} -8 & 16 \\ 28 & -12 \end{pmatrix} \equiv \begin{pmatrix} 21 & 16 \\ 28 & 17 \end{pmatrix} \bmod 29. \end{aligned}$$

Check: Modulo 29, we have

$$\begin{pmatrix} 3 & 4 \\ 7 & 2 \end{pmatrix} \begin{pmatrix} 21 & 16 \\ 28 & 17 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Hill Cipher

Example (continued)

Suppose you want to encrypt the message:

“THE FOOL ON THE HILL.”

Encrypting T $= 19$ and H $= 7$ modulo 29:

$$\begin{pmatrix} 3 & 4 \\ 7 & 2 \end{pmatrix} \begin{pmatrix} 19 \\ 7 \end{pmatrix} = \begin{pmatrix} -2 \\ 2 \end{pmatrix} = \begin{pmatrix} 27 \\ 2 \end{pmatrix} = \begin{pmatrix} , \\ \mathsf{C} \end{pmatrix}.$$

Decrypting , $= 27$ and C $= 2$ modulo 29:

$$\begin{pmatrix} 21 & 16 \\ 28 & 17 \end{pmatrix} \begin{pmatrix} 27 \\ 2 \end{pmatrix} = \begin{pmatrix} -10 \\ 7 \end{pmatrix} = \begin{pmatrix} 19 \\ 7 \end{pmatrix} = \begin{pmatrix} \mathsf{T} \\ \mathsf{H} \end{pmatrix}.$$

Hill Cipher

Example (continued)

The following table shows the encryption of this plaintext with key A.

plaintext	T H	E □	F O	O L	□ O	N □	T H	E □	H I	L L
plaintext encoded	19 7	4 26	5 14	14 11	26 14	13 26	19 7	4 26	7 8	11 11
ciphertext encoded	27 2	0 22	13 5	28 4	18 7	27 27	27 2	0 22	24 7	19 12
ciphertext	, C	A W	N F	. E	S H	, ,	, C	A W	Y H	T M

Permutation Cipher

Theorem

The permutation cipher is linear.

Proof: Let $\pi \in \mathfrak{S}_n$ be a permutation. Let $U_n = (\vec{u}_i)_{1 \leq i \leq n}$ be the $(n \times n)$ unity matrix whose i^{th} row is $\vec{u}_i$, the i^{th} unity vector of length n.

Let M_π be the matrix whose i^{th} row is $\vec{u}_{\pi(i)}$.

This matrix can be obtained from U_n by permutating its rows according to π. Hence,

$$(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}) = M_\pi \vec{x}$$

for each vector $\vec{x} = (x_1, x_2, \ldots, x_n)$ in Σ^n. ❑

Corollary

The permutation cipher is a special case of the Hill cipher.

Kasiski's Method: Cryptanalysis of the Vigenère Cipher

- This method was invented by Friedrich Wilhelm Kasiski in 1863. It was also invented, independently, by Charles Babbage (around 1854, unpublished).

- If the period is known, the problem of breaking the polyalphabetic cryptosystem can be reduced to the problem of breaking a monoalphabetic cryptosystem by the method of frequency counts.

Example:

- Suppose that the period is $n = 7$.
- Arrange the ciphertext $C_0 C_1 C_2 \cdots C_k$, where each C_j is a letter, in seven columns such that the i^{th} column consists of the letters C_j with subscript $j \in \{i, i+7, i+2 \cdot 7, \ldots\}$, where $i \in \mathbb{Z}_7$ and $j \leq k$.

Kasiski's Method: Cryptanalysis of the Vigenère Cipher

C_0	C_1	C_2	C_3	C_4	C_5	C_6
C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}
C_{14}	C_{15}	C_{16}	C_{17}	C_{18}	C_{19}	C_{20}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
C_{k-8}	C_{k-7}	C_{k-6}	C_{k-5}	C_{k-4}	C_{k-3}	C_{k-2}
C_{k-1}	C_k					

Table: Cryptanalysis of a polyalphabetic system with period 7

- Apply the method of frequency counts to each single column.

Kasiski's Method: Cryptanalysis of the Vigenère Cipher

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

Table: Kasiski's method: ciphertext obtained by the Vigenère cipher

Kasiski's Method: Cryptanalysis of the Vigenère Cipher

- Suppose you have intercepted the ciphertext shown in the table on the previous slide, and you know that it has been encrypted by the Vigenère cipher.
- The ciphertext has 373 letters, and you do not know the period (i.e., the length of the key) used.
- Analyzing the ciphertext carefully, you will find that some sequences of letters occur repeatedly in the text.
- Some of these repeated three-letter patterns are highlighted using different colors in the table on the next slide.

Kasiski's Method: Cryptanalysis of the Vigenère Cipher

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

Table: Kasiski's method: three-letter patterns occurring repeatedly in the text

Kasiski's Method: Cryptanalysis of the Vigenère Cipher

- If one such pattern occurs repeatedly, this can be
  - either due to the fact that the same plaintext string was encrypted using the same letters of the key,
  - or it may be a pure coincidence.
- Suppose it is not coincidental.

  Hence, the *distance between repeatedly occurring patterns* will tell you something about the *key length* used.
- By "*distance*" we mean the number of positions some pattern has to be shifted to coincide with another one. For example,
  - the pattern "**A H O**" occurs three times with distances 20 and 30;
  - the pattern "**U Y D**" occurs three times with distances 55 and 125;
  - the pattern "**A C D**" occurs twice with distance 30;
  - the pattern "**I H R**" occurs twice with distance 20;
  - the pattern "**B L D**" occurs twice with distance 165.

Kasiski's Method: Cryptanalysis of the Vigenère Cipher

Determine the block length:

- If the repeated occurrence of a pattern is no coincidence, then the key length (i.e., the period of the system) must divide all distances.
- For example, a distance of 20 means that the period is either 2 or 4 or 5 or 10 or 20.
- Since also 30 is a distance between patterns, the potential periods 4 and 20 are eliminated.
- Among the remaining possible periods, 2 and 5 and 10, only the period 5 divides the distances 55, 125, and 165.
- Thus, we have determined the key length 5.

Kasiski's Method: Cryptanalysis of the Vigenère Cipher

Determine the key:

- Now we can try to find the key and to decipher the message.
- Knowing the period, we can reduce this task to the task of breaking a monoalphabetic system by frequency counts.
- Rearranging the ciphertext in five columns, we obtain five monoalphabetic encryptions.
- In particular, the second column has 75 letters, see the table on the next slide.

Kasiski's Method: Cryptanalysis of the Vigenère Cipher

Determine the key:

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

Table: Kasiski's method: second column of the ciphertext rearranged

- Note that the letter "**E**" occurs most frequently: 14 times (10.5%).
- But this means that the letters in the second column have not been encrypted at all! Analyzing the fifth column gives the same result.
- Thus, the second and the fifth letter of the key is an "**A**."
- Continuing in this way, we finally obtain the key used: "**PAULA**."

Kasiski's Method: Cryptanalysis of the Vigenère Cipher

Decipher the ciphertext:

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

Kasiski's Method: Cryptanalysis of the Vigenère Cipher

Decipher the ciphertext:

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

Kasiski's Method: Cryptanalysis of the Vigenère Cipher

Decipher the ciphertext:

key	P	A	U	L	A	P	A	U	L	A	P	A	U	L	A	P	A	U	L	A

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

Kasiski's Method: Cryptanalysis of the Vigenère Cipher

Decipher the ciphertext:

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

Kasiski's Method: Cryptanalysis of the Vigenère Cipher

We had great fun in Spain that year and we travelled and wrote and Hemingway took me tuna fishing and I caught four cans and we laughed and Alice Toklas asked me if I was in love with Gertrude Stein because I had dedicated a book of poems to her even though they were T.S. Eliot's and I said, yes, I loved her, but it could never work because she was far too intelligent for me and Alice Toklas agreed and then we put on some boxing gloves and Gertrude Stein broke my nose.

Woody Allen, *A Twenties Memory*,
Random House, Inc., 1971

Cryptanalysis of the Affine Linear Block Cipher

Affine Linear Block Ciphers can be broken by *known-plaintext attacks*:

- Suppose that some key $(A, \vec{b})$ has been fixed, that is, the plaintext $\vec{x} \in \mathbb{Z}_m^n$ is encrypted as
$$\vec{y} = E_{(A,\vec{b})}(\vec{x}) = A\vec{x} + \vec{b} \bmod m,$$
where A is an $(n \times n)$ matrix over $\mathbb{Z}_m$ with $\mathtt{gcd}(\det A, m) = 1$, and $\vec{y}$ and $\vec{b}$ are vectors in $\mathbb{Z}_m^n$.
- Suppose we know $n+1$ plaintexts $\vec{x}_0, \vec{x}_1, \ldots, \vec{x}_n$ and the corresponding ciphertexts $\vec{y}_0, \vec{y}_1, \ldots, \vec{y}_n$ with
$$\vec{y}_i = A\vec{x}_i + \vec{b} \bmod m.$$
- It follows that
$$\vec{y}_i - \vec{y}_0 \equiv A(\vec{x}_i - \vec{x}_0) \bmod m. \tag{6}$$

Cryptanalysis of the Affine Linear Block Cipher

- Define the matrices X and Y by

$$\begin{aligned} X &= (\vec{x}_1 - \vec{x}_0, \vec{x}_2 - \vec{x}_0, \ldots, \vec{x}_n - \vec{x}_0) \bmod m; \\ Y &= (\vec{y}_1 - \vec{y}_0, \vec{y}_2 - \vec{y}_0, \ldots, \vec{y}_n - \vec{y}_0) \bmod m. \end{aligned}$$

  That is,

  - the i^{th} column of X is the difference $\vec{x}_i - \vec{x}_0 \bmod m$, and
  - the i^{th} column of Y is the difference $\vec{y}_i - \vec{y}_0 \bmod m$,

  where $1 \leq i \leq n$.

- It follows from (6) that

$$AX \equiv Y \bmod m.$$

Cryptanalysis of the Affine Linear Block Cipher

- If $\det X$ is coprime to m, then

$$X^{-1} = (\det X)^{-1} X_{\texttt{adj}},$$

where $(\det X)^{-1}$ denotes the inverse of $\det X$ mod m.

- Thus, we have

$$A \equiv Y((\det X)^{-1} X_{\texttt{adj}}) \bmod m.$$

- Furthermore, since

$$\vec{b} = (\vec{y}_0 - A\vec{x}_0) \bmod m,$$

we have determined the key $(A, \vec{b})$ from $n+1$ pairs of plaintexts and corresponding ciphertexts.

Cryptanalysis of Linear Block Ciphers and the Hill Cipher

- If the cryptosystem is even linear, then $\vec{b} = \vec{0}$, and we may choose
$$\vec{x}_0 = \vec{y}_0 = \vec{0}.$$
- In particular, if $n = 2$, the Hill cipher can be broken when two pairs, (x_1, y_1) and (x_2, y_2), are known.
- For example, suppose you have intercepted two pairs of plaintexts and corresponding ciphertexts, say the first two blocks of the encryption by the Hill cipher given in our previous example.

Cryptanalysis of Linear Block Ciphers and the Hill Cipher

- The following table shows these two known pairs:

$$\vec{x}_1 = (19,7) \quad \text{and} \quad \vec{y}_1 = (27,2), \text{ and}$$
$$\vec{x}_2 = (4,26) \quad \text{and} \quad \vec{y}_2 = (0,22).$$

plaintext	T	H	E	□
plaintext encoded	19	7	4	26
ciphertext encoded	27	2	0	22
ciphertext	,	C	A	W

Table: Breaking the Hill cipher with a known-plaintext attack

Cryptanalysis of Linear Block Ciphers and the Hill Cipher

- Thus, you obtain the matrices $X = \begin{pmatrix} 19 & 4 \\ 7 & 26 \end{pmatrix}$ and $Y = \begin{pmatrix} 27 & 0 \\ 2 & 22 \end{pmatrix}$.
- Since

$$\det X = 19 \cdot 26 - 4 \cdot 7 = 2$$

and $m = 29$ are coprime, you further obtain $(\det X)^{-1} = 15$ and

$$X_{\mathtt{adj}} = \begin{pmatrix} 26 & -4 \\ -7 & 19 \end{pmatrix} \equiv \begin{pmatrix} 26 & 25 \\ 22 & 19 \end{pmatrix} \bmod 29.$$

Cryptanalysis of Linear Block Ciphers and the Hill Cipher

- Hence, the key used can be deciphered by

$$\begin{aligned} A &\equiv Y\left((\det X)^{-1} X_{\mathtt{adj}}\right) \bmod 29 \\ &\equiv \begin{pmatrix} 27 & 0 \\ 2 & 22 \end{pmatrix} \left(15 \begin{pmatrix} 26 & 25 \\ 22 & 19 \end{pmatrix}\right) \bmod 29 \\ &\equiv \begin{pmatrix} 27 & 0 \\ 2 & 22 \end{pmatrix} \begin{pmatrix} 13 & 27 \\ 11 & 24 \end{pmatrix} \bmod 29 \\ &\equiv \begin{pmatrix} 3 & 4 \\ 7 & 2 \end{pmatrix} \bmod 29. \end{aligned}$$

Triple Encryption

- The security of a block cipher can be increased by applying it repeatedly with distinct keys.
- This measure can increase the key space considerably. A common way of doing so is the *triple encryption*. After choosing three keys, say k_1, k_2, and k_3, a given plaintext x is encrypted by

  $$y = E_{k_1}(D_{k_2}(E_{k_3}(x))),$$

  where E_{k_i} are the encryption functions and D_{k_i} the decryption functions for k_i. The ciphertext y can then be decrypted by

  $$x = D_{k_3}(E_{k_2}(D_{k_1}(y))).$$

Electronic Codebook Mode (ECB)

- Suppose we are given a block cipher with block length n.
- Messages are strings in Σ^*, where Σ is an alphabet. The key space is K.
- To encode a plaintext m in the *electronic codebook mode (ECB)*, subdivide it into blocks of length n:

  $$\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_k,$$

  where the last block may have to be padded by random letters to ensure that n divides $|m|$.

Electronic Codebook Mode (ECB)

- If $e \in K$ is the encryption key, every block of length n is encrypted by e:

$$\vec{c}_i = E_e(\vec{b}_i), \quad 1 \leq i \leq k.$$

- The ciphertext is the resulting sequence of ciphertext blocks:

$$c = \vec{c}_1 \ \vec{c}_2 \ \cdots \ \vec{c}_k.$$

- If $d \in K$ is the decryption key corresponding to e, the ciphertext blocks are decrypted with d one after another, yielding the original plaintext:

$$m = D_d(\vec{c}_1) \ D_d(\vec{c}_2) \ \cdots \ D_d(\vec{c}_k).$$

- All previous examples of block ciphers have been encrypted in the ECB mode.

Electronic Codebook Mode (ECB): Disadvantages

1. The same plaintext blocks are encrypted into the same ciphertext blocks. Thus, regularities in the plaintext yield regularities in the ciphertext. A cryptanalysist can exploit this information obtained from the ciphertext, which may be sufficient to break the cipher.

   For instance, in the previous example for how to break the Vigenère cipher by Kasiski's method, the highlighted ciphertext patterns "**A H O**," "**U Y D**," and "**A C D**" each encrypt the plaintext "**A N D**," which results from using the ECB mode for the Vigenère cipher.

2. An attacker can easily tamper with the encrypted messages by
   - deleting ciphertext blocks,
   - inserting additional ciphertext blocks, or
   - altering the order of the ciphertext blocks.

Cipherblock Chaining Mode (CBC)

- The *cipherblock chaining mode (CBC)* avoids the disadvantages of the ECB mode by working in a “context-sensitive” way: The encryption of a plaintext block in the CBC mode depends not only on the block being encrypted and the key, but also on preceding blocks.
- Hence, depending on their context, identical patterns in the plaintext are encrypted differently.
- If an attacker was tampering with the ciphertext, it can no longer be decrypted properly, which reveals that someone was trying to do something nasty.
- The CBC mode is explained for the permutation cipher.

Cipherblock Chaining Mode (CBC)

- Let $\Sigma = \{0,1\}$ be an alphabet, n be the block length, and $\mathfrak{S}_n$ be the key space (of the permutation cipher). Let E_π be the encryption function and $D_{\pi^{-1}}$ be the decryption function for key $\pi \in \mathfrak{S}_n$.
- Define the logical *exclusive-or* operation $\oplus : \{0,1\}^2 \to \{0,1\}$ by its truth table:

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

- For $\vec{x}, \vec{y} \in \{0,1\}^n$ with $\vec{x} = (x_1, x_2, \ldots, x_n) = x_1 x_2 \cdots x_n$ and $\vec{y} = (y_1, y_2, \ldots, y_n) = y_1 y_2 \cdots y_n$, let

$$\vec{x} \oplus \vec{y} = (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n) = x_1 \oplus y_1 \;\, x_2 \oplus y_2 \;\, \cdots \;\, x_n \oplus y_n.$$

Cipherblock Chaining Mode (CBC)

- To encode a plaintext m in the *cipherblock chaining code (CBC)*, subdivide it into blocks of length n (assuming n divides $|m|$):
$$\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_k.$$
- Choose an initial vector $\vec{c}_0 \in \{0,1\}^n$.
- For $\pi \in \mathfrak{S}_n$, every block $\vec{b}_i$ is encrypted as follows:
$$\vec{c}_i = E_\pi(\vec{c}_{i-1} \oplus \vec{b}_i), \quad 1 \leq i \leq k.$$
- The ciphertext is the resulting sequence of ciphertext blocks:
$$c = \vec{c}_1 \ \vec{c}_2 \ \cdots \ \vec{c}_k.$$
- For $\pi^{-1} \in \mathfrak{S}_n$, every ciphertext block $\vec{c}_i$ is decrypted by:
$$\vec{b}_i = \vec{c}_{i-1} \oplus D_{\pi^{-1}}(\vec{c}_i), \quad 1 \leq i \leq k.$$

Cipherblock Chaining Mode (CBC): Disadvantages

- The receiver has to wait for the next ciphertext block before starting with the decryption.
- These delays result in a certain inefficiency, in particular if the block length is large.

This disadvantage can be avoided by the *cipher feedback mode (CFB)*.

Cipher Feedback Mode (CFB)

Idea:

- Subdivide the message into blocks *shorter* than the block length n of the block cipher used.
- Do not use only the block cipher's own encryption function, but encrypt these shorter blocks by adding certain key blocks modulo 2.
- These key blocks can almost simultaneously be generated by the sender and the receiver of the ciphertext.
- The CFB mode is again explained for the permutation cipher.

Cipher Feedback Mode (CFB)

- Consider the permutation cipher with alphabet $\Sigma = \{0,1\}$, block length n, and key space $\mathfrak{S}_n$. Let $\pi \in \mathfrak{S}_n$ the encryption key.
- Choose some k with $1 \leq k \leq n$ and an initial vector $\vec{z}_0 \in \{0,1\}^n$.
- Subdivide message m into $d = \lceil {}^{|m|}/_{k} \rceil$ blocks $\vec{b}_1, \vec{b}_2, \dots, \vec{b}_d$ of length k. For each i with $1 \leq i \leq d$:

  Step 1: Compute $\vec{x}_i = E_\pi(\vec{z}_{i-1})$.

  Step 2: Let $\vec{y}_i$ be the string in $\{0,1\}^k$ consisting of the first k bits of $\vec{x}_i \in \{0,1\}^n$.

  Step 3: Compute $\vec{c}_i = \vec{b}_i \oplus \vec{y}_i$.

  Step 4: Compute $\vec{z}_i = 2^k \vec{z}_{i-1} + \vec{c}_i \bmod 2^n$, i.e., the first k bits are deleted in $\vec{z}_{i-1}$ and $\vec{c}_i$ is attached as a suffix.

- The resulting ciphertext consists of the blocks $\vec{c}_1, \vec{c}_2, \dots, \vec{c}_d$.

Cipher Feedback Mode (CFB)

Example: Let $n = 5$ and $k = 4$, and consider the message

$$m = 10011\ 10101\ 01001\ 00100.$$

- Subdivide the message into five blocks of length k:
$$\vec{b}_1 = 1001,\ \vec{b}_2 = 1101,\ \vec{b}_3 = 0101,\ \vec{b}_4 = 0010,\ \vec{b}_5 = 0100.$$
- If $\pi = \binom{1\ 2\ 3\ 4\ 5}{3\ 5\ 1\ 2\ 4} \in \mathfrak{S}_5$ is our key and $\vec{z}_0 = 11010$ our initial vector, we encrypt these blocks as follows:

i	$\vec{b}_i$	$\vec{x}_i$	$\vec{y}_i$	$\vec{c}_i$	$\vec{z}_i$
0	—	—	—	—	11010
1	1001	00111	0011	1010	01010
2	1101	00011	0001	1100	01100
3	0101	10010	1001	1100	01100
4	0010	10010	1001	1011	01011
5	0100	01011	0101	0001	10001

Cipher Feedback Mode (CFB)

- Decryption works almost like the encryption. The only difference occurs in the third step. For each i with $1 \leq i \leq d$:

  Step 1: Compute $\vec{x}_i = E_\pi(\vec{z}_{i-1})$.

  Step 2: Let $\vec{y}_i$ be the string in $\{0,1\}^k$ consisting of the first k bits of $\vec{x}_i \in \{0,1\}^n$.

  Step 3: Compute $\vec{b}_i = \vec{c}_i \oplus \vec{y}_i$.

  Step 4: Compute $\vec{z}_i = 2^k \vec{z}_{i-1} + \vec{c}_i \bmod 2^n$, i.e., the first k bits are deleted in $\vec{z}_{i-1}$ and $\vec{c}_i$ is attached as a suffix.

- The decrypted message obtained consists of the blocks $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_d$.

Cipher Feedback Mode (CFB)

Remark:

- Both the sender and the receiver can determine $\vec{y}_1$ as soon as the initial vector $\vec{z}_0$ is chosen.
- Then, the sender computes $\vec{c}_1 = \vec{b}_1 \oplus \vec{y}_1$ and sends it, and the receiver computes $\vec{b}_1 = \vec{c}_1 \oplus \vec{y}_1$.
- Then, they can both determine $\vec{y}_2$, and so on.
- **Advantage (in comparison with the CBC mode):** The block length k can be much shorter than the actual block length n.

  $\Longrightarrow$ less idle time during which the receiver has to wait for the sender, so both can encrypt and decrypt almost simultaneously.

Output Feedback Mode (OFB)

- The *output feedback mode (OFB)* is quite similar to the CFB mode:
  - The initialization and
  - the first three steps of both the encryption and the decryption procedure are identical.
  - The only difference occurs in the fourth step, which determines the vector $\vec{z}_i$ for $1 \leq i \leq d$.

- For encryption, the OFB mode works as follows:

  Step 1: Compute $\vec{x}_i = E_\pi(\vec{z}_{i-1})$.

  Step 2: Let $\vec{y}_i$ be the string in $\{0,1\}^k$ consisting of the first k bits of $\vec{x}_i \in \{0,1\}^n$.

  Step 3: Compute $\vec{c}_i = \vec{b}_i \oplus \vec{y}_i$.

  Step 4: Compute $\vec{z}_i = \vec{x}_i$.

Output Feedback Mode (OFB)

Example: Let $n = 5$ and $k = 4$. The block encryption in the CFB mode shown in the previous example gives the following block encryption in the OFB mode for the same message $m = 10011\ 10101\ 01001\ 00100$, subdivided into five blocks of length k:

$$\vec{b}_1 = 1001,\ \vec{b}_2 = 1101,\ \vec{b}_3 = 0101,\ \vec{b}_4 = 0010,\ \vec{b}_5 = 0100,$$

the same key $\pi = \binom{1\ 2\ 3\ 4\ 5}{3\ 5\ 1\ 2\ 4} \in \mathfrak{S}_5$, and the same initial vector $\vec{z}_0 = 11010$:

i	$\vec{b}_i$	$\vec{x}_i$	$\vec{y}_i$	$\vec{c}_i$	$\vec{z}_i$
0	—	—	—	—	11010
1	1001	00111	0011	1010	00111
2	1101	11001	1100	0001	11001
3	0101	01110	0111	0010	01110
4	0010	10011	1001	1011	10011
5	0100	01101	0110	0010	01101

Output Feedback Mode (OFB)

- Decryption works again almost like the encryption. The only difference occurs in the third step:

  Step 3: Compute $\vec{b}_i = \vec{c}_i \oplus \vec{y}_i$.

Remark: **Advantage (in comparison with the CFB mode):**

- If there are transmission errors in the ciphertext of a message encrypted in the OFB mode, then this error occurs after decryption only at exactly the same position.
- In contrast, transmission errors in ciphertexts encrypted in the CFB mode occur after decryption as long as it takes to shift the erroneous block out of the vector $\vec{z}_i$, which depends on the block lengths n and k.

Stream Ciphers

- The principle of the CBC mode is generalized by the notion of a *stream cipher*.
- Stream ciphers generate a continuous stream of keys such that each key may depend on the preceding keys and on the context of the plaintext already encrypted.
- We now introduce a popular stream cipher that is based on a *linear feedback shift register*, and thus explains the general idea of stream ciphers.

Stream Cipher Based on a Linear Feedback Shift Register

- Let $\Sigma = \{0,1\}$ be the alphabet used. Σ^* is both the plaintext space and the ciphertext space. For fixed $n \in \mathbb{N}$, the key space is Σ^n.
- Any message $\vec{m} = m_1 m_2 \cdots m_z$ in Σ^* is encrypted symbol by symbol as follows.
- Suppose that $z \geq n$. Given a key $\vec{k} = (k_1, k_2, \ldots, k_n)$ in Σ^n, generate a key stream $\vec{s} = (s_1, s_2, \ldots, s_z, \ldots)$, initialized by $\vec{k}$ for the first n bits:

$$s_i = k_i \qquad \text{for } 1 \leq i \leq n,$$

and continuing according to the following linear recursion of order n:

$$s_i = \sum_{j=1}^{n} a_j s_{i-j} \bmod 2 \qquad \text{for } i > n, \tag{7}$$

where $a_1, a_2, \ldots, a_n \in \{0,1\}$ are fixed coefficients.

Stream Cipher Based on a Linear Feedback Shift Register

- Denoting the first z bits of the key stream $\vec{s}$ by $\vec{s}(z)$, the encryption function $E_{\vec{k}}$ and the decryption function $D_{\vec{k}}$, both mapping from Σ^* to Σ^*, are defined by:

$$\begin{aligned} E_{\vec{k}}(\vec{m}) &= \vec{m} \oplus \vec{s}(|\vec{m}|); \\ D_{\vec{k}}(\vec{c}) &= \vec{c} \oplus \vec{s}(|\vec{c}|), \end{aligned}$$

  where $\oplus$ denotes the addition of bit vectors modulo 2.

  That is, the i^{th} bit of $\vec{m} \oplus \vec{s}$ is $m_i \oplus s_i$, the exclusive-or of m_i and s_i.

Stream Cipher Based on a Linear Feedback Shift Register

Example:

- For a concrete example, let $n = 5$, and fix the coefficients $a_1 = a_3 = a_4 = 0$ and $a_2 = a_5 = 1$.
- Then, the key stream $\vec{s}$ is generated by the recursion

$$s_{i+5} = s_{i+3} + s_i \bmod 2. \tag{8}$$

- Choosing the key $\vec{k} = (1, 0, 0, 1, 1)$, one obtains

$$\vec{s} = (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, \ldots).$$

- The linear recursion from (8) can be efficiently realized by a building block of hardware, namely a linear feedback shift register as shown on the next slide.

Stream Cipher Based on a Linear Feedback Shift Register

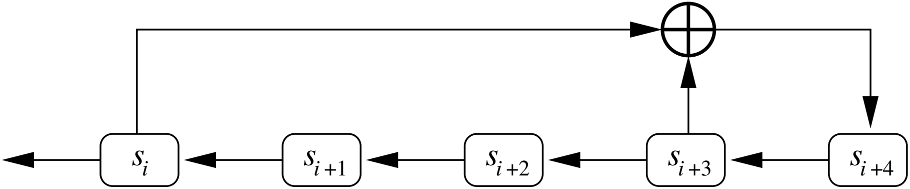

Figure: A linear feedback shift register

- The registers store the last four bits of the key stream $\vec{s}$ generated.
- In each recursion step, the bit from the leftmost register is used as the current key. Then, the bits from the other registers are shifted by one position to the left.
- The rightmost register is now fed the bit that results from adding modulo 2 the bits from those registers with coefficient $a_i = 1$.

Stream Cipher Based on a Linear Feedback Shift Register

Known-Plaintext Attack for Breaking this Stream Cipher:

- This attack is similar to the cryptanalysis of affine linear block ciphers such as the Hill cipher.
- Note that all operations used in this stream cipher are linear.
- Thus, knowing a string of plaintext and a corresponding string of ciphertext, you can solve a system of linear equations to determine the values of the n unknown coefficients in the linear recursion (7).

Stream Cipher Used in the Enigma

- This stream cipher realizes one of the ideas from the infamous encryption machine *Enigma* that the Deutsche Wehrmacht used during World War II.

- The key space is $\mathbb{Z}_{26}$.

- For some fixed key $k \in \mathbb{Z}_{26}$ and for each $i \geq 1$, generate the key stream $\vec{s}$ by defining its i^{th} element by the rule

$$s_i = (k + i - 1) \bmod 26.$$

Stream Cipher Used in the Enigma

- Let π be some fixed permutation of $\mathbb{Z}_{26}$.
- If $s \in \mathbb{Z}_{26}$ is the current element of the key stream and x is the current plaintext letter, the encryption function E_s, which maps from $\mathbb{Z}_{26}$ to $\mathbb{Z}_{26}$, uses both π and s as follows:

$$E_s(x) \quad = \quad \pi((x+s) \bmod 26).$$

- Similarly, the decryption function D_s, which also maps from $\mathbb{Z}_{26}$ to $\mathbb{Z}_{26}$, uses both s and the inverse permutation π^{-1} to decrypt the current ciphertext symbol y:

$$D_s(y) \quad = \quad (\pi^{-1}(y) - s) \bmod 26.$$

Stream Cipher Used in the Enigma: A Puzzle

Suppose that the permutation π of $\mathbb{Z}_{26}$ is given by

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 \\ 11 & 8 & 6 & 1 & 3 & 4 & 5 & 9 & 10 & 2 & 7 & 0 & 14 & 12 & 20 & 13 & 25 & 21 & 15 & 17 & 24 & 18 & 16 & 22 & 19 & 23 \end{pmatrix}.$$

The following ciphertext was produced by the above stream cipher with π:

FRRMXCBEWMJWDDH TKO UACYKUK QAMT ASVZWO

- Find the key used by exhaustive search of the key space,
- determine the complete key stream, and
- decrypt the ciphertext.