BA2 AICC2 Résumé

Probability

$\Omega = \{w_1, .., w_n\}$ sample space (set of outcomes), E: event (subset of Ω) $p(E) = \frac{|E|}{|\Omega|} = \sum_{w \in E} p(w)$, $p(E|F) = \frac{|E \cap F|}{|F|} = \frac{p(E \cap F)}{p(F)} = \frac{p(F|E)\,p(E)}{p(F)}$ (Bayes' Rule), probability distribution: $p: \Omega \to [0,1]$ st. $\sum_{w \in \Omega} p(w) = 1$

$p(E|F) = p(E) \Leftrightarrow$ E and F are independant, $p(E \cap F) = p(E) \cdot p(F) \Leftrightarrow$

$p(E \cup F) = p(E) + p(F) \Leftrightarrow$ disjoint events, $p(E) = p(E|F) \cdot p(F) + p(E|F^c) \cdot p(F^c)$ (law total probability; complement of F), Random var. X: Func. $X: \Omega \to \mathbb{R}$, probability distribution $p_X(x) = \sum_{w \in E} p(w)$ with $E = \{w \in \Omega : X(w) = x\}$, marginal distribution $p_X(x) = \sum_y p_{X,Y}(x,y)$

expected value $\mathbb{E}[X] = \sum_w X(w)p(w) = \sum_x x\, p_X(x)$, X and Y independant iff. $p_{X,Y}(x,y) = p_X(x)\, p_Y(y)$ (for all realizations), $p_{Y|X}(y|x) = \frac{p_{X,Y}(x,y)}{p_X(x)}$ (conditional distribution), $p(x,y,z) = p(x) \cdot p(y|x) \cdot p(z|x,y)$, $p(w,z) = p(w)\, p(z|w)$

$\Rightarrow \mathbb{E}[XY] = \mathbb{E}[X] \cdot \mathbb{E}[Y]$ iff. $p_{Y,X}(y|x) = p_Y(y)$ iff. $p_{X|Y}(x,y) = p_X(x)$

Entropy

$H_b(S) = -\sum_{s \in supp(p_S)} p_S(s) \log_b(p_S)$, $supp = \{s : p_S(s) > 0\}$, $H(S) = -\sum_{s \in A} p_S(s) \log_2 p_S(s) = \mathbb{E}[-\log_2 p_S(S)]$ (A ← alphabet; linear), Uniform distribution $(p_S(s) = \frac{1}{|A|})$ $H(S) = \log_2|A|$ → max. entropy, $h(p) := -p\log_2 p - (1-p)\log_2(1-p)$ binary entropy Func. $(|A| = 2)$, $h(\varepsilon) = h(1-\varepsilon)$, $H(S)$ when $p = 1/2$ $h(p) = 1$ (max.), (IT-Ineq.) $\log_b r \leqslant (r-1)\log_b e$ = iff. $r = 1$

$0 \leqslant H_b(S) \leqslant \log_b |A|$

= iff. $\exists s\ p_S(s) = 1$; = iff. $p_S(s) = \frac{1}{|A|}\ \forall s$ (Uniform)

Source coding

Encoder(A, D, C, Γ) (input alphabet, output alphabet, D^m codebook, 1 to 1 map: $A^k \to C$), uniquely decodable $\Leftrightarrow \forall$ concatenation of codewords $\exists!$ parsing into seq. of codewords, $\Leftrightarrow$ its reverse is uniq. deco., = instantaneous code prefix-free $\Rightarrow$ uniq. deco., Fixe-length $\Rightarrow$ uniq. deco., $\neg$Kraft $\neg(\sum D^{-l_i} \leqslant 1) \Rightarrow \neg$uniq. deco. $\Rightarrow$ has prefix, D-ary code uniq deco. $\Rightarrow D^{-l_1} + \ldots + D^{-l_m} \leqslant 1 \Leftrightarrow$ (Kraft-MM) $\exists$ D-ary prefix-free code with lengths (codeword lengths)

$L(S, \Gamma) = \sum_{s \in A} p_S(s)\, l(\Gamma(s))$ (average codeword length, length), uni deco. $\Rightarrow H_D(S) \leqslant L(S,\Gamma)$, Shannon-Fano $l(\Gamma(s)) = \lceil -\log_D p_S(s) \rceil$ (=iff $p(s) = D^{-l(\Gamma(s))}\ \forall s$) $H_D(S) \leqslant L(S, \Gamma_{SF}) < H_D(S) + 1$, Huffman → tree (prefix free, optimal, $\sum p_i l_i = \sum q_i$ nodes) $L(S, \Gamma_H) \leqslant L(S, \Gamma)$, recursively connect 2 lowest leafs,

Conditional Entropy

$H_D(X,Y) = -\sum_{(x,y)} p(x,y) \log_D(p(x,y))$ (joint), X,Y independent $\Leftrightarrow p(x,y) = p(x) \cdot p(y)$, $\Leftrightarrow H(Y|X) = H(Y) \Leftrightarrow H(X,Y) = H(X) + H(Y)$, per-letter average $H(S) \leqslant \frac{L((S_1,S_2,..,S_n),\Gamma_{SF})}{n} < H(S) + \frac{1}{n}$ ($n \to \infty$), $p(x|y) = \frac{p(x,y)}{p(y)}$ (knowing y occured), $0 \leqslant H(X|Y) \leqslant \log|\mathcal{X}|$, $H(X|Y=y)$, $x \in \mathcal{X}$

$H(Y|X) \leqslant H(Y)$ = iff. independent, $H(S_1,...,S_n) = H(S_1) + H(S_2|S_1) + H(S_3|S_1,S_2) + \ldots + H(S_n|S_1,...,S_{n-1})$

$p(x\|y)$ ($\neq p(y\|x)$)	$y=0$	$y=1$
$x=0$	$1-\varepsilon$	δ
$x=1$	ε	$1-\delta$

$H(X|Y)$

$p(x,y)$	$y=0$	$y=1$	
$x=0$	$\frac{1}{2}(1-\varepsilon)$	$\frac{1}{2}\delta$	$p(x)$
$x=1$	$\frac{1}{2}\varepsilon$	$\frac{1}{2}(1-\delta)$	
	$p(y)$		marginals

$H_D(X|Y=y) = -\sum_x p(x|y) \log_D(p(x|y))$, $H(X|Y) = \sum_y p(y) H(X|Y=y)$, $H(X|Y) \leqslant H(X) \leqslant H(X,Y) \leqslant H(X) + H(Y)$, $H(X,Y) = H(X) + H(Y|X)$, $H(S_1,S_2,..,S_n) \leqslant H(S_1) + H(S_2) + \ldots + H(S_n)$, $\Rightarrow H(Y|X) = H(X,Y) - H(X)$, $H(F(X)|X) = 0$ (F is a Func), $H(X|F(X)) = 0$ (F is 1-to-1), Sunny-Rainy Source: (sun ⇄ rain) tomorrow's weather only depends on today's

Source Coding Theorem

Source $S = (S_1, S_2, \ldots)$ (sources), entropy of a symbol $H(S) = \lim_{n\to\infty} H(S_n)$, entropy rate $H^*(S) = \lim_{n\to\infty} H(S_n|S_1,S_2,..,S_{n-1})$ (non-increasing in n), S is regular iff. $H(S) \wedge H^*(S)$ exist and finite, Coin-Flip Source $p(S_1, .., S_n) = \frac{1}{2^n}$, Stationary ($n \to \infty$) iid. sources

distribution stay the same when shifted in time (indexes)

Stationary Source: $\forall n,k \in \mathbb{N}^*$ $(S_1,...,S_n)$ same statistics as $(S_{k+1},...,S_{k+n})$, Stationary ⇒ Regular $H^*(S) \leqslant H(S)$ (= if symbols are independent), $\lim_{n\to\infty} \frac{H_D(S_1,S_2,...,S_n)}{n} = H_D^*(S)$ ⇒ good measure of information minimum average codeword length, $\frac{H_D(S_1,..,S_n)}{n} = H_D(S_1)$, $\frac{H_D(S_1,..,S_n)}{n} \to H(S_n|S_1,..,S_n)$

Cryptography

$t \to E_{K_A}(t) \to c \to D_{K_B}(c) \to t$ (plaintext, encrypt, cipher, key, decrypt), Caesar: $c_i = t_i + k \pmod{|A|}$, $t_i = c_i - k \pmod{|A|}$, $k \in A$, monoalphabetic: permutation (caesar is any alphabet; Fixed substitution table $A \to \gamma$, $B \to v$), $k \in A^n$ $t_i = c_i - k_{i \bmod n} \pmod{|A|}$, Vignère: $c_i = t_i + k_{i \bmod n} \pmod{|A|}$, One-Time Pad: $c_i = t_i \oplus k_i$, $t_i = c_i \oplus k_i$, $t, k \in \{0,1\}^n$, k ← uniform & independant source, k should be used only once ($k = c \oplus t$)

Vigenère, One-Time Pad (public)

Polyalphabetic: mutiple substitution tables, Ciphertext-only: encrypted with same K (one or more C known), Known plaintext: encrypted with same K (one or more (t,c) pairs), chosen plaintext: under the same k (get C given any t), perfect secrecy: independent (t and c statistically) $\Rightarrow H(t) \leqslant H(k)$

Symmetric-key: $K_A = K_B = k$, Diffie Hellman: arithmetic is mod p: Fixed large prime, g: generator (g^i generates $\{1,..,p-1\}$, $\{0,..,p-2\}$), a,b secret, $A = g^a$ $B = g^b$ public, $K = A^b = B^a = g^{ab}$, hard to compute $\log(A)$ and $\log(B)$ (discrete exponentiation), One-Way Func.: → fast ← slow, Trapdoor One-Way: → fast ← slow, ← Fast (trapdoor info.),

ElGamal: x,y random & secret, g^y, g^x public, Alice(x), Bob(y), $t \to c = g^{yx} t \to t = i \cdot c$, compute i: mutiplicative inverse (mod p) of g^{yx}, change x,y for each transaction,

Mod

$a = bq + r$ (dividend, divisor, quotient, remainer) $0 \leqslant r < |b|$, (8 mod 3 = 2, −8 mod 3 = 1, 8 mod −3 = 2, −8 mod −3 = 1), congruence: $a \equiv b \pmod m \Leftrightarrow m | a-b$ (divides) $\Leftrightarrow (a-b) \bmod m = 0$, $\Leftrightarrow a \bmod m = b \bmod m$, $a \equiv a' \pmod m$, $b \equiv b' \pmod m$ $\Rightarrow$ $a + b \equiv a' + b' \pmod m$, $ab \equiv a'b' \pmod m$, $a^n \equiv (a')^n \pmod m$, $\mathbb{P}$: primes, prime: $p \in \mathbb{N}$ $p > 1$ no positive divisor other than 1 and itself, composites: non-primes

$\forall x \in \mathbb{N}$ $x > 1$ $\exists!$ prime factorization, $a|b \Leftrightarrow \exists c \in \mathbb{Z}: b = a \cdot c$, $\gcd(a,b)$: largest $x \in \mathbb{N}$ st. $x|a$ and $x|b$ (greatest common divisor), coprime (relatively/mutually prime): $\gcd(a,b) = 1$, $p \in \mathbb{P}$ $a \in \mathbb{N}^*$ $a < p \Rightarrow \gcd(p,a) = 1$, $a|c$, $b|c$, $\gcd(a,b) = 1 \Rightarrow ab|c$; $ab|c \Rightarrow a|c$ and $b|c$

$[a]_m$: congruent class of a mod. m ($m \in \mathbb{N}$ $m > 1$; integers congruent to a (mod m)), $[a]_m = [b]_m$ iff. $a \equiv b \pmod m$, $\mathbb{Z}/m\mathbb{Z}$: Set of every $[a]_m$ ("$\mathbb{Z}$ mod m" $/\mathbb{Z}_m$ $\{0,1,...,m-1\}$ $\{1,...,m\}$ unique), reduced form: $[r]_m$ ($0 \leqslant r \leqslant m-1$), $[a]_m + [b]_m = [a+b]_m$, $[a]_m \cdot [b]_m = [a \cdot b]_m$, $k[a]_m = [ka]_m$ ($= [k]_m[a]_m$), multiplicative inverse i: $[a]_m[i]_m = [i]_m[a]_m = [1]_m$ does not always exist

$(([a]_m)^{-1})^{-1} = [a]_m$ (inverse), $([a]_m)^0 = [1]_m$, $[a]_m$ ($\in \mathbb{Z}/m\mathbb{Z}$) has a mult. inverse iff. $\gcd(a,m) = 1$, p prime ⇒ all elements have inverse except $[0]_p$, $\gcd(a,b) = \gcd(b, a - kb)$ ($a,b \in \mathbb{Z}^*$, $\forall k \in \mathbb{Z}$) $\exists u,v \in \mathbb{Z}$ $\gcd(a,b) = au + bv$, Mod 97-10: $c = X \& (98 - (X \& 00 \bmod 97))$ (verifg: c mod 97 = 1)

Groups

Abelian commutative group: a set G with a binary operation $*$ st ① $\forall a,b \in G$ $a*b \in G$ (closure) ② $\forall a,b$ $a*(b*c) = (a*b)*c$ (associativity) ③ $\exists e \in G$ st. $\forall a \in G$ $a*e = a$ (identity element) ④ $\forall a \in G$ $\exists i \in G$ st. $a*i = a$ (inverse element) ⑤ $\forall a,b \in G$ $a*b = b*a$ (commutativity)

$\mathbb{Z}/m\mathbb{Z}^*$: elements of $\mathbb{Z}/m\mathbb{Z}$ that have a mult. inverse, $(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$ is a commutative group, Euler's $\phi(n)$: number of integers in $[1,n]$ relatively prime to n, $\phi(m) = |\mathbb{Z}/m\mathbb{Z}^*|$, $\phi(p) = p-1$, $\phi(p^k) = p^k - p^{k-1}$ ($p,q \in \mathbb{P}$, $\forall k \in \mathbb{N}^*$), $\phi(pq) = \phi(p) \cdot \phi(q)$ $= (p-1)(q-1) = pq - p - q - 1$

$G = G_1 \times G_2$ $(G, *)$ $(a_1,a_2) * (b_1,b_2) = (a_1 *_1 b_1, a_2 *_2 b_2)$ (product operation), cartesian product of a commutaive group is a commutative group, $(G, \times)$ and $(H, \otimes)$ isomorphic iff. $\exists$ bijection $V: G \to H$ st. $V(a \times b) = V(a) \otimes V(b)$, $V(e_G) = e_H$, $a \times a^{-1} = e_G \Rightarrow V(a) \otimes V(a^{-1}) = e_H$

order of a: smallest k st. $a^k = \underbrace{a \times a \times \ldots \times a}_{k \text{ times}} = e$, $a^m = e$ iff. $k|m$ ($a^m = a^{m \bmod k}$), G Finite ∧ commutative with $|G| = n$: $\forall a \in G$ $\exists k \in \{1,..,n\}$ ← divisors of n, 2 Finite commutative groups are isomorphic iff. they have same set of orders, $\forall a \in \mathbb{Z}/m\mathbb{Z}^*$ $a^{\phi(m)} = [1]_m$, $\forall a \in \mathbb{Z}/p\mathbb{Z}$ $a^p = a$ (p: a prime)

RSA

chinese remainders $\psi: \mathbb{Z}/m_1m_2\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$, $\gcd(m_1,m_2) = 1 \Rightarrow$ $[k]_{m_1m_2} \to ([k]_{m_1}, [k]_{m_2})$ bijective ∧ isomorphic with "+" "·", p q (distinct) primes k: mutiple of $(p-1) \wedge (q-1)$ ($\mathrm{lcm}(p-1,q-1)$) $([a]_{pq})^{l \cdot k + 1} = [a]_{p \cdot q}$ $\forall l \in \mathbb{N}$,

$\gcd(m_2, m_1) = 1 \leftarrow [k]_{m_1m_2} = [m_2 [m_2]^{-1}_{m_1} [k]_{m_1} + m_1 [m_1]^{-1}_{m_2} [k]_{m_2}]_{m_1m_2}$

RSA: (receiver) ① large primes $p\ q \rightarrow m = p \cdot q$ (modulus) ② k: multiple of $(p-1)$ and $(q-1)$ ($k=\phi(p,q)$ or $k=\text{lcm}(p-1,q-1)$) ③ e (encoding exponent, $e=65537$ prime) st. $\gcd(e,k)=1 \rightarrow d$: $d\,e + k \cdot L = 1$ (Bézout) ($[e]_k^{-1}$) ④ public key: (m,e) private key: (m,d), $([t]_m^e)^d = [t]_{pq}^{ed} = [t]_{pq}^{1-kL} = [t]_m$ (cipher), send (t,s)

hash: maps long to fixed length - hard to find y st. $h(x)=h(y)$ (many-to-one function, given $h(x)$), digital signature: $s = f^{-1}(h(t))$ (reverse trapdoor one-way) verify $h(t)=f(s)$

Cyclic groups: $\exists g \in G$ st $G = \{g, g^2, \ldots, g^n = e\}$ (générateur), $a \in G$ is a generator iff. order of $a = |G|$, a cyclic group G has $\phi(|G|)$ generators, discrete exp.: base b $f: \mathbb{Z}/n\mathbb{Z} \rightarrow G$ $[i]_n \mapsto b^i$, f: isomorphism from $(\mathbb{Z}/n\mathbb{Z},+)$ to $(G,*)$ iff G is cyclic $\wedge$ b is a generator $\Rightarrow$ discrete log: base b $f^{-1}: G \rightarrow \mathbb{Z}/n\mathbb{Z}$ $a = b^i \mapsto [i]_n$,

inverse of $[b]_m \in (\mathbb{Z}/m\mathbb{Z}^*, \cdot)$: ① Bézout $\gcd(b,m) = 1 = b \cdot u + m \cdot v \Rightarrow [b]_m^{-1} = [u]_m$ ($[m]_b^{-1} = [v]_b$) $(\gcd(b,r)$ with a,b: $q = a // b$ | $r = a \% b$ | $u = \tilde{v}$ | $v = \tilde{u} - q\tilde{v})$ (0, 1) ② $[b]_m^{\phi(m)} = 1 \Rightarrow [b]_m^{-1} = [b]_m^{\phi(m)-1}$ or $[b]_m^{\text{order}(b)-1}$ cyclic group: $b^{-1} = b^{|G|-1}$

Errors: error 1001, erasure $0?11$, weight: nb. of errors, code C: set of codewords, codeword $c \in A^n$ ($(c_1, c_2, \ldots, c_n)$, alphabet), block-length: n, $k := \log_2|C| = \log_{|A|}|C|$ (bits/codeword, information/codeword), rate: $R = \frac{k}{n}$, Hamming dist: $d(x,y)$ nb. of differences, minimum-dist decoder: $\hat{c} = \arg\min_{x \in C} d(c,x)$ (x st.),

min. dist.: $d_{min}(C) = \min_{x,y \in C;\, x \neq y} d(x,y)$, error detection channel: $p < d_{min}$, error correction $p < \frac{d_{min}}{2}$, erasure correction channel: $p < d_{min}$, $d_{min} \leqslant n-k+1$ (= iff MDS ← min. dist separable code),

Finite Fields: Field: $(K,+,\times)$ $\forall a,b,c \in K$ $\exists$ identities: 0 for $+$, 1 for $\times$; $a+(b+c)=(a+b)+c$, $a \times (b \times c) = (a \times b) \times c$; $a+b=b+a$, $a \times b = b \times a$; $a+0=a$, $a \times 1 = a$; $\exists!(-a): a+(-a)=0$ (additive inverse); $a \neq 0 \Rightarrow \exists!\, a^{-1}: a \cdot a^{-1} = 1$ (multiplicative inverse); $a \times (b+c) = (a \times b) + (a \times c)$; $(K,+)$ and $(K \setminus 0, \times)$ are commut. groups; Finite Field: K finite, $a - b := a + (-b)$, $ab := a \times b$, $n\,b := b + b + \ldots + b$ (n times, $\in \mathbb{N}$), $b^n := b \times b \times \ldots \times b$,

$x \in K \setminus 0: x \cdot y = 0 \Rightarrow y = 0$; $x \in K \Rightarrow x\,0 = 0 \wedge x^m = 0 \Rightarrow x = 0$, $(-1) \cdot x = -x$, $(a+b)^2 = a^2 + 2ab + b^2$, characteristic of a finite field: order of 1 with respect to $+$ $\rightarrow$ prime number p, $\exists m \in \mathbb{N}: |F| = p^m$, (Finite field) $|F_1| = |F_2| \Rightarrow F_1, F_2$ isomorphic, $(\mathbb{Z}/p\mathbb{Z},+,\times)$ is a finite field iff. p is prime, F_{p^m}: field with p^m elements, $\forall a \in F_{p^m} \setminus 0$ order$(a,+) = p$, $\forall a \in F$ $p\,a = 0$,

Vector Spaces: V over F (non-empt set, finite field): $\vec{u}, \vec{v} \in V$ add $\vec{u} + \vec{v} \in V$, $\alpha, \beta \in F$ scal. mult. $\alpha \times \vec{v} \in V \rightarrow \times$: $(V,+)$: commutative group, $\alpha(\beta\vec{v}) = (\alpha\beta)\vec{v}$, $1\vec{v} = \vec{v}$, $\alpha(\vec{u}+\vec{v}) = \alpha\vec{u} + \beta\vec{v}$, $(\alpha+\beta)\vec{v} = \alpha\vec{v} + \beta\vec{v}$, $V = F^n$: n-tuples, subspace: $S \subseteq V$ closed under $+$, $\times$ scal., linear comb. of n vectors: $\sum_{i=1}^{n} \lambda_i \vec{v}_i$ ($\in F$), span of vectors: set of all linear comb., $\text{span}(\vec{v}_1, \ldots, \vec{v}_2) = V$ (spans V),

V finite dimensional: finite list of vectors spans V, n vectors are linearly independent: $\sum_{i=1}^{n} \lambda_i \vec{v}_i = \vec{0} \Rightarrow \vec{\lambda} = \vec{0}$, Basis of V (lin. indep. vectors span V): $(\vec{v}_1, \ldots, \vec{v}_n)$ st. $\forall \vec{v} \in V$ $\exists!\,\vec{\lambda}$ (unique): $\vec{v} = \sum_{i=0}^{n} \lambda_i \vec{v}_i$, every base have same length: $\dim V$, solutions in $V = F^n$ of m linear homog. equat. M (← span of coef. vectors) in n variables subset S of $V \rightarrow \dim S = n - \dim M$, rank of matrix: $\dim(\text{span}(\text{rows})) = \dim(\text{span}(\text{columns}))$,

$V = F^n \Rightarrow$
$|V| = |F^n| = |F|^n$

Linear Codes code words (C) $\rightarrow$ k-dimentional subspace of F^n (some finite field), linear code $\Rightarrow$ (contrapositive to prove non linear) $|C| = |F|^k$ (number of codewords), Hamming weight: $w(\vec{x}) = d(\vec{0}, \vec{x})$ ($\in F^n$; number of non-zero components), $d_{min}(C) = \min_{\vec{c} \in C \setminus \vec{0}} w(\vec{c})$, (only) Binary (linear) MDS codes: Parity-check: $C = \{\vec{c} \in F_2^n : \sum_i c_i = 0\}$ | Repetition: $\{\vec{0}, \vec{1}\}$ | F_2^n,

generator matrix: $G = \begin{pmatrix} \vec{c}_1 \\ \vdots \\ \vec{c}_k \end{pmatrix}$ ($k \times n$; B^T) for linear code $C \subseteq F^n$ with basis $(\vec{c}_1, \ldots, \vec{c}_k)$, G: encoding map (!use row vectors) $\vec{u} \mapsto \vec{c} = \vec{u}G$ ($\vec{u} \in F^k$, $\vec{c} \in F^n$), systematic codes have a systematic form: $G_s = (I_k \| P_{k \times (n-k)})$ (row reduce G) $\rightarrow$ encodes to $(\vec{u}$, validation$)$ swap columns changes the code but not (n, k, d_{min}),

parity check matrix: $H \in F^{(n-k) \times n}$ defines homogeneous equations that code words respect: $\vec{c}H^T = \vec{0}$ iff. $\vec{c} \in C$ $H_{(s)} = (-P^T \| I_{n-k})$ (concatenate), $G_s H^T = 0$, syndrome: $\vec{s} = \vec{y}H^T$ (received ~code word) column in H where error happened, $d_{min}(C)$: $\min\{d \in \mathbb{N} : d$ columns of H are linearly dependent$\}$,

$[a] = a * G$ ("translated" G), $D_i = c_i + D_0$ (coset leader (min weight))

Reed Solomon Codes: $\vec{u} \in F^k \rightarrow P_{\vec{u}}(x) = \sum_{i=1}^{k} u_i x^{i-1}$ (polynomial, $\in F$), (n,k) RS ($0 < k \leqslant n \leqslant |F|$): $(a_1, \ldots, a_n)$ distinct ($\in F$) $\vec{u} \rightarrow \vec{c} = (P_{\vec{u}}(a_1), \ldots, P_{\vec{u}}(a_n))$ ($F^k \rightarrow F^n$), RS codes are linear and MDS $\Rightarrow d_{min} = n-k+1$, $G = \begin{pmatrix} a_1^0 & \cdots & a_n^0 \\ \vdots & & \vdots \\ a_1^{k-1} & \cdots & a_n^{k-1} \end{pmatrix}$

@gruvw

Cryptography

plaintext → encrypt, cipher, key, decrypt, public

$t \to E_{K_A}(t) \to c \to D_{K_B}(c) \to t$

Caesar: $k \in A$, $c_i = t_i + k \pmod{|A|}$, $t_i = c_i - k \pmod{|A|}$

Monoalphabetic: any alphabet permutation — Fixed substitution table (A→P, B→V, ⋮)

Vignère: $k \in A^n$, $c_i = t_i + k_{i \bmod n} \pmod{|A|}$, $t_i = c_i - k_{i \bmod n} \pmod{|A|}$

One-Time Pad: $t, k \in \{0,1\}^n$, k ← uniform & independant source, $c_i = t_i \oplus k_i$, $t_i = c_i \oplus k_i$

k should be used only once ($k = c \oplus t$)

Polyalphabetic: mutiple substitution tables

Ciphertext-only: one or more c known encrypted with same k

Known plaintext: one or more (t,c) pairs encrypted with same k

Chosen plaintext: get c given any t under the same k

Perfect secrecy: t and c statistically independent $\Rightarrow H(t) \leqslant H(k)$

Diffie Hellman: g: generator (g^i generates $\{1, \dots, p-1\}$, $i \in \{0, \dots, p-2\}$)

arithmetic is mod p: Fixed large prime

a, b secret

$A = g^a$ $B = g^b$ public

$K = A^b = B^a = g^{ab}$

hard to compute $\log(A)$ and $\log(B)$ → discrete exponentiation

One-Way Func.: → Fast, ← slow

Trapdoor One-Way: → Fast, ← slow, ← trapdoor info. Fast

ElGamal: x, y random & secret, g^y, g^x public

Alice$^{(x)}$: $t \to c = g^{yx} t \to$ Bob$^{(y)}$: $t = i \cdot c$

compute i: mutiplicative inverse (mod p) of g^{yx}

change x,y for each transactions

@gruvw

Mod

dividend, divisor, quotient, remainer: $a = bq + r$ $\quad 0 \leqslant r < |b|$

divides: $a | b \Leftrightarrow \exists c \in \mathbb{Z} : b = a \cdot c$

$[a]_m$: congruent class of a mod. m ($m \in \mathbb{N}$, $m > 1$; integers congruent to a (mod m))

$[a]_m$ ($\in \mathbb{Z}/m\mathbb{Z}$) has a mult. inverse iff. $\gcd(a, m) = 1$

Congruence: $a \equiv b \pmod{m} \Leftrightarrow m | a - b \Leftrightarrow (a-b) \bmod m = 0 \Leftrightarrow a \bmod m = b \bmod m$ (divides)

$ab | c \Rightarrow a | c$ and $b | c$

$a | c, b | c, \gcd(a,b) = 1 \Rightarrow ab | c$

$[a]_m + [b]_m = [a+b]_m$

$[a]_m \cdot [b]_m = [a \cdot b]_m$

$a, b \in \mathbb{Z}^*$, $\forall k \in \mathbb{Z}$: $\gcd(a,b) = \gcd(b, a - kb)$

$a \equiv a' \pmod{m}$, $b \equiv b' \pmod{m}$ $\Rightarrow$ $a + b \equiv a' + b' \pmod{m}$, $ab \equiv a'b' \pmod{m}$, $a^n \equiv (a')^n \pmod{m}$

$\gcd(a,b)$: largest $x \in \mathbb{N}$ st. $x | a$ and $x | b$

Coprime: $\gcd(a,b) = 1$

multiplicative inverse i: $[a]_m [i]_m = [i]_m [a]_m = [1]_m$

$\exists u, v \in \mathbb{Z}$ $\gcd(a,b) = au + bv$

$[a]_m = [b]_m$ iff. $a \equiv b \pmod{m}$

$\mathbb{P}$: primes

prime: $p \in \mathbb{N}$ $p > 1$ no positive divisor other than 1 and itself

$p \in \mathbb{P}$ $a \in \mathbb{N}^*$ $a < p \Rightarrow \gcd(p, a) = 1$

$\mathbb{Z}/m\mathbb{Z}$ ("Z mod m" / $\mathbb{Z}_m$): Set of every $[a]_m$

Groups

@gruvw

Abelian

commutative group: a set G with a binary operation $*$

① closure: $\forall a,b \in G \quad a*b \in G$

② associativity: $\forall a,b \quad a*(b*c)=(a*b)*c$

③ identity element: $\exists e \in G$ st. $\forall a \in G \quad a*e=a$

④ inverse element: $\forall a \in G \; \exists i \in G$ st. $a*i=a$

⑤ commutativity: $\forall a,b \in G \quad a*b=b*a$

$G=G_1 \times G_2 \quad (G,*) \quad (a_1,a_2)*(b_1,b_2)=(a_1 *_1 b_1, a_2 *_2 b_2)$ (product operation)

$\mathbb{Z}/m\mathbb{Z}^*$: elements of $\mathbb{Z}/m\mathbb{Z}$ that have a mult. inverse

$(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$ is a commutative group $\quad \phi(n)=|\mathbb{Z}/m\mathbb{Z}^*|$

Euler's $\phi(n)$: number of integers in $[1,n]$ relatively prime to n

$p,q \in \mathbb{P} \quad \forall k \in \mathbb{N}^* \quad \phi(p)=p-1, \; \phi(p^k)=p^k-p^{k-1}, \; \phi(pq)=\phi(p)\cdot\phi(q)$ $=(p-1)(q-1)=pq-p-q-1$

cartesian product of a commutaive group is a commutative group

Errors:

@gruvw

erasure 0?11

error 1001

weight: nb. of errors

code C: set of codewords

codeword $c \in A^n$ — $(c_1,c_2,..,c_n)$, A: alphabet

block-length: n

rate: $R=\frac{k}{n}$

$k := \log_2|C| := \log_{|A|}|C|$ (bits/codeword, information/codeword)

Hamming dist $d(x,y)$: nb. of differences

minimum-dist decoder: $\hat{c} = \arg\min_{x \in C} d(c,x)$

min. dist.: $d_{min}(C)=\min_{x,y \in C;\, x \neq y} d(x,y)$

error channel: detection $p < d_{min}$ — correction $p < \frac{d_{min}}{2}$

erasure channel: correction $p < d_{min}$

$d_{min} \leqslant n-k+1$ ($=$ iff MDS ← min. dist separable code)

@gruvw

Linear Codes

code words (C) → k-dimentional subspace of F^n (some finite field)

linear code ⇒ $|C| = |F|^k$ (number of codewords) (contrapositive to prove non linear)

Hamming weight: $w(\vec{x}) = d(\vec{0}, \vec{x})$ ($\vec{x} \in F^n$) — number of non-zero components

$d_{min}(C) = \min_{\vec{c} \in C \setminus \vec{0}} w(\vec{c}) = \min \{ d \in \mathbb{N} : d \text{ columns of } H \text{ are linearly dependent} \}$ (linear)

(only) Binary MDS codes. Parity-check: $C = \{ \vec{c} \in F_2^n : \sum_i c_i = 0 \}$ | Repetition. $\{\vec{0}, \vec{1}\}$ | F_2^n

generator matrix: $G = \begin{pmatrix} \vec{c}_1 \\ \vdots \\ \vec{c}_k \end{pmatrix}$ ($k \times n$, B^T) For linear code $C \subseteq F^n$ with basis $(\vec{c}_1, \ldots, \vec{c}_k)$

G: encoding map $\vec{u} \mapsto \vec{c} = \vec{u} G$ ($\vec{u} \in F^k$, $\vec{c} \in F^n$)

systematic codes have a systematic form. $G_s = (I_k \| P_{k \times (n-k)})$ (row reduce G) → encodes to $(\vec{u}, \text{validation})$

swap columns changes the code but not (n, k, d_{min})

parity check matrix: $H \in F^{(n-k) \times n}$ defines homogeneous equations that code words respect. $\vec{c} H^T = \vec{0}$ iff. $\vec{c} \in C$ $H_{(s)} = (-P^T \| I_{n-k})$

$G_s H^T = 0$

syndrome: $\vec{s} = \vec{y} H^T$ (received ~code word) — column in H where error happened