

Index

- .. XPath abbreviation, 113
 - . XPath abbreviation, 113–114
 - // XPath abbreviation, 113
 - @ XPath abbreviation, 113
- A**
- Abbreviated location paths, 108
 - Absolute location paths, 107–108
 - Absolute URIs, 204
 - Abstract elements, 96
 - Abstract types, 96
 - Actor attribute, 150–151
 - Actors, 150, 152–153
 - Addison-Wesley Internet Web site, xviii
 - Addition (+) operator, 116
 - Adjunct meaning, 472–473
 - AES (Advanced Encryption Standard)
 - algorithms, 410
 - AES (Advanced Encryption Standard), 18
 - AES Key Wrap algorithms, 416–420
 - AES-128 algorithm, 391
 - AES-128 Key Wrap algorithm, 391
 - AES-192 algorithm, 391
 - AES-192 Key Wrap algorithm, 391
 - AES-256 algorithm, 391
 - AES-256 Key Wrap algorithm, 391
 - Agreement data as content, 316
 - AgreementMethod element, 296, 298, 308,
 - 316–317, 366–367, 387, 395, 398–401, 402–403
 - AgreementMethod algorithms, 214, 385
 - AgreementMethod role element, 386
 - Algorithm attribute, 383
 - Algorithmic pseudo-random number
 - generators, 30
 - Algorithmic roles, 385–394
 - Algorithms, 213–214
 - AES (Advanced Encryption Standard), 410
 - AES Key Wrap, 416–420
 - applications, 385
 - ARCFOUR, 411
 - Base-64 Decoding, 424–425
 - block encryption, 408–410
 - Canonical XML, 422–423
 - canonicalization, 421–424
 - CMS Key Checksum, 414
 - Diffie-Hellman Key Agreement, 401–404
 - DSA, 406–407
 - encryption, 369
 - Enveloped Signature Transform, 430
 - Exclusive XML Canonicalization, 423
 - explicit parameters, 383
 - HMAC SHA-1, 405
 - HMAC variations of, 406
 - implicit inputs or parameters, 383
 - key agreement, 398–404
 - key transport, 412–414
 - MAC (Message Authentication Code),
 - 404–406
 - MDS, 395–397
 - message digest, 395–398
 - Minimal Canonicalization, 423–424
 - non-cryptographic, 421–433
 - RIPEMD-160, 398
 - RSA variations of, 408
 - RSA Version 1.5, 412–413
 - RSA-OAEP, 413–414
 - RSA-SHA1, 407–408
 - SHA versions of, 397–398
 - SHA-1, 397
 - signature, 406–408
 - stream encryption, 410–411
 - style of URIs, 385, 387
 - symmetric key wrap, 414–420
 - syntax, 383–384
 - text-based canonicalization, 217
 - transform, 424–433
 - Triple DES, 409–410
 - Triple DES Key Wrap, 415–416
 - XML Schema Validation, 432–433
 - XML-based canonicalization, 217
 - XPath Filtering, 425–430

- Algorithms (*cont.*)
 - XPointer, 431–432
 - XSLT Transform, 430–431
- Algorithm-specific namespaces, 383
- Amount of processing, 473
- Amp (&) escape string, 53
- Ampersand (&) character (&), 42, 52–53, 63, 187
- Ancestor, 74
- ancestor:: axis, 109, 137
- ancestor-or-self:: axis, 109, 137
- And Boolean operator, 115
- Anonymous actor, 150
- Anonymous type, 94
- ANY content model, 75
- ANY keyword, 75
- anyAttribute element, 353
- anyType data type, 94, 271
- anyURI simpleType, 89
- Apache Web site, 438–439
- Apache Xalan package, 438–439
- Apex element, 150
- Apos (') escape string, 53
- Application-defined keys, 299
- Applications, 35
 - algorithms, 385
 - context, 247
 - digital signature algorithms, 252
 - DTD elimination, 204
 - equivalences and canonicalization, 201–202
 - executable content, 252
 - mapping parameter names into XML, 165
 - PIs (processing instructions), 54–55
 - processing instruction, 84
 - retrieval method, 322
 - XML Digital Signature standard, 422
 - XML Encryption standard, 346
- Arbitrary-length integers, 213, 302
- ARCFOUR algorithm, 391, 411
- Arithmetic algorithm division, 384
- Arithmetic operators, 116–117
- ASCII format, 462–463
- ASN.1 BER SHA1 algorithm designator prefix, 407–408
- Assures element, 254–256
- Asymmetric key ciphers, 19–20
- Asymmetric keys and authentication, 20–21
- attribute:: axis, 109, 137
- Attribute nodes, 104, 196–197
- attributeFormDefault attribute, 95
- Attribute-list declaration, 70
- Attributes, 47–48
 - alphabetic order, 194
 - beginning name with letter, 82
 - case of name, 82
 - covering range, 138
 - default, 184
 - default values, 82–83
 - DTDs (Document Type Definitions), 79–82
 - end tags, 82
 - fixed values, 83
 - global, 92
 - groups of, 94
 - local, 92–93
 - missing, 93
 - name, 47
 - null value, 93
 - optional, 83
 - ordering, 186
 - qualifying names, 56, 58
 - required, 83
 - restricting value of, 80–81
 - schemas, 91–95
 - simpleType, 89
 - SOAP, 149
 - special, 48–50
 - special properties, 69
 - start tags, 79
 - surrounding values with quotes, 82
 - types, 79–81, 184
 - unique values, 97
 - unordered, 173
 - value delimiters, 186–187
 - value normalization, 183–184
 - values, 47, 93
 - white space between, 173
 - xmlns: prefix, 57
- Audio markup, 38
- Authentication, 8, 207
 - asymmetric keys, 20–21
 - paper point of view, 476
 - protocol point of view, 476–477
- Authentication codes, 207
- AuthInfo element, 333
- Authorities, 124–126
- AuthServerInfo element, 332
- AuthServerInfoType element, 337–338
- AuthUserInfoType element, 336

- Automatic transforms, 243–244
- Axis, 108
- B**
- Baltimore Technologies Web site, 439, 442
- Baltimore Technologies XMLDSIG product Web site, 439
- Bare name XPointers, 242
- Bare names, 135
- Base URIs (Uniform Resource Identifiers), 130–132, 204
- Base64 algorithm, 394
- Base-64 Decoding algorithms, 424–425
- Base-64 encoded certificate revocation list, 310
- Base-64 encoded Key Material Packet, 314
- Base-64 encoded plain value, 309
- Base-64 Transform element, 425
- base64Binary simpleType, 89, 213
- BCP (Best Current Practice) standard, 461
- Berners-Lee, Tim, 453
- Big endian, 213
- Bignums, 213, 302
- Binary data, 60
- Binary ISO public key infrastructure items, 272
- Block encryption algorithms, 408–410
- Body element, 37, 70, 151
- Boolean functions, 121
- Boolean operators, 115–116
- Boolean() function, 114, 121
- Bottom attribute, 93
- Bottom-level user certificates, 24
- Boxing patents, 11
- Boyer, John, 170
- Browser-oriented processor, 40
- Browsers and semantic attacks, 126
- BSAFE Cert-J SDK Web site, 449
- Byte objects, xxi–xxii
- C**
- Candidate Recommendation, 454
- Canonical XML, 10, 169–170, 205, 218, 365, 421, 439
 - ancestor environment characteristics, 197
 - applying to node-set, 176
 - comments, 230
 - explicit interoperability testing, 437
 - input/read rules, 182–184
 - namespace declarations output, 189
 - namespace nodes output, 198
 - output/print rules, 184–188
 - Unicode character normalization, 202
 - UTF-8 character encoding, 185
 - with and without comments, 192
 - XML encryption, 178–180
 - XPath expressions, 242
- Canonical XML algorithms, 218, 388, 422–423
- Canonical XML and Exclusive Canonical XML for Python Web site, 450
- Canonical XML for Perl Web site, 447
- Canonical XML interoperability matrix Web site, 437
- Canonical XML with Comments algorithm, 388
- Canonicalization, 29, 477
 - alphabetic order for namespaces and attributes, 194
 - application equivalences, 201–202
 - attribute and namespace ordering, 186
 - attribute nodes, 196–197
 - attribute types, 204
 - attribute value delimiters, 186–187
 - attribute value normalization, 183–184
 - CDATA sections, 182–183
 - character normalization, 202–203
 - comment nodes, 199–200
 - custom, 188, 201, 205
 - definition of, 169
 - digital signatures, 249
 - do nothing, 218
 - document encoding, 185
 - document order, 193
 - element nodes, 195–196
 - empty elements, 186
 - encryption, 421
 - essential for digital signatures over XML, 171–178
 - exclusive/inclusion of ancestor namespace declarations, 205–206
 - formal generative specification, 194–200
 - inclusion of default attributes, 184
 - inherited attribute and namespace declaration rules, 188–190
 - input/read rules, 182–184
 - limitations, 200–206
 - line breaks, 182
 - minimal, 218
 - namespace declaration inheritance and superfluous declaration deletion, 188–190

- Canonicalization (*cont.*)
 - namespace nodes, 197–198
 - node-sets, 192–193
 - normalizing namespace prefixes, 175
 - notations, 85, 204
 - operational nonequivalence, 203–204
 - output/print rules, 184–188
 - paper point of view, 475
 - processing instruction nodes, 199
 - protocol point of view, 475–476
 - reference replacement, 182
 - relative URIs, 204
 - removing XML declaration and DTD, 182
 - requirement for XML data, 178
 - root node, 195
 - signatures, 421
 - SOAP, 260
 - special characters in text output encoded, 187
 - text nodes, 198–199
 - transformative summary, 180–190
 - unparsed external entities, 204
 - well-formed XML, 194–195
 - white space
 - in content, 187
 - inside start and end tags, 187
 - outside document, 185
 - in processing instructions, 187
 - XML, 172–173
 - xml namespace attributes, 188, 205–206
 - XPath data model, 190–191
 - XPath node, 192
- Canonicalization algorithms, 421–424
- Canonicalization data model, 190–194
- Canonicalization of XML, 460
- CanonicalizationMethod algorithm, 213, 217, 393
- CanonicalizationMethod element, 216–219, 246, 247, 406, 421
 - flexibility, 218
 - P3P (Platform for Privacy Preferences), 258
- CanonicalizationMethod role element, 386, 387
- Canonicalized Reference element, 248
- Canonicalized SignatureMethod, 247
- Canonicalized SignedInfo, 247
- Capslock Ubisecure Signature XMLDSIG
 - product Web site, 442
- Capslock Web site, 442
- Cardinality indicator characters, xxi
- Carriage return (`xOD`), 183
- Carriage return new line (`xODxOA`), 182
- CarriedKeyName element, 354–355, 364, 366
- Case sensitivity, 41
- CBC (Cipher Block Chaining) mode, 409
- CDATA sections, 50–51, 182–183
- CDATA type, 184
 - attributes, 80
 - termination string, 50
- ceiling() function, 122
- Certificate references, 285
- Certificates
 - assurance about public key, 22
 - authenticating digital signature, 23
 - chain of, 23
 - containing validation key, 310
 - date of issuance and expiration, 23
 - hierarchical model, 23–24
 - identity or access authorization, 23
 - mesh model, 24
 - OCSF (Online Certificate Status Protocols), 26–27
 - PGP (Pretty Good Privacy), 25
 - public key, 23
 - revocation lists, 25–26
 - status of, 314
 - type supported, 331
 - X.509, 25
 - X.509v3, 25
- CertificateValues element, 288–289, 291
- Certification authorities, 23
- Certs element, 275
- CGI (Common Gateway Interface) programs, 127
- Channels, 334
- Character content, 105–106
- Character data, 50–51, 80
- Character Map, 53
- Character normalization, 202–203
- Character references, 182–183
- Character sets, 52–53
- Character-point preceding node, 139
- Characters
 - alphabetic comparisons, 194
 - appending to normalized value, 183
- Checksum, 14
- child:: axis, 109, 137
- Child elements, 45, 78–79

- Child sequence XPointers, 242
 - Child sequences, 135
 - Cipher text, 17
 - base-64 encoded octet, 350
 - decryption, 410–411
 - encryption, 410–411
 - reference to external location, 350–352
 - CipherData elements, 348, 350–353, 359, 364, 366–367, 414
 - CipherReference element, 344, 350–352, 366–367, 393, 424
 - Ciphers, 17–18
 - CipherValue element, 344, 350–351, 364, 366–367
 - Circumflex (^), 132
 - Clark, James, 35
 - Client and server sample code (ASP .NET)
 - Web site, 447
 - Clients
 - authorized to register key, 336
 - data elements requested by, 327
 - generating key pair, 332
 - information about keys, 322
 - validity of assertion, 324
 - CMS (Cryptographic Message Syntax) Key
 - Checksum, 414
 - CMS Key Checksum algorithms, 414
 - CMS (Cryptographic Message Syntax) of
 - S/MIME, 412
 - Collapsed ranges, 138
 - Comment nodes, 107, 199–200
 - ::comment() node test, 111
 - Comments, 51–52
 - Canonical XML, 230
 - Exclusive XML Canonicalization, 230
 - preserving, 190
 - CommitmentTypeId element, 280
 - CommitmentTypeIndication element, 279–280
 - CommitmentTypeQualifiers element, 280
 - Compatibility between XML documents, 6
 - CompleteCertificateRefs element, 284–285, 291
 - CompleteRevocationRefs element, 285–287, 291
 - Complex form digital signatures example, 237–239
 - Complex protocol digital signature example, 234–236
 - Complex types, deriving types from, 97
 - complexType construct, 89
 - complexType element, 90
 - Concatenating strings, 119
 - concat() function, 119
 - Confidentiality, 9
 - Construct, 90
 - Container nodes, 136–137
 - Containers, 136
 - contains() function, 119
 - Content, restricting, 94–95
 - Content model elements, 74–77
 - ContentTimeStamp element, 283–284
 - Context, 114, 142
 - Context node, 120
 - Core meaning, 471, 472
 - CounterSignature element, 277–278
 - count() function, 117
 - Covering range, 141
 - CRL (certificate revocation lists), 26, 285
 - CrIcspRef element, 287
 - CRLValues, 289–290
 - Cryptographic algorithms and XKMS, 334–338
 - Cryptography
 - asymmetric key ciphers, 19–20
 - MACs (message authentication codes), 15–17
 - message digests, 13–15
 - public key ciphers, 19–20
 - secret key ciphers, 17
 - symmetric key ciphers, 17–18
 - CSS (Cascading Style Sheets), 64–65, 67
 - Custom canonicalization, 188, 201, 205
 - Customized markup languages, 35
- D**
- Data
 - decrypting, 408–410
 - digest of, 214–215
 - digital signatures, 214–215
 - encrypting, 361–362, 408–410
 - information about, 215–216
 - MIME type, 225–227
 - multiple keys, 227
 - SignatureMethod algorithms, 227
 - specifying which is signed, 220–224
 - standard form of, 169
 - subset, 132

- Data (*cont.*)
 - transforms, 222
 - type pointed to, 221–222
 - verification has failed, 227
- Data objects, 36
- Data structures, 40
- Data types
 - abstract, 96
 - deriving from complex types, 97
 - listing, 97
 - restricting derivation, 97
 - schemas, 89–90, 213
 - specifications, 96
 - XAdES signatures, 271–273
- DataEncodingUnknown faults, 153
- DataObjectFormat element, 278–279
- DataReference elements, 356, 358
- dateTime simpleType, 89
- Decimal character references, 53
- Decrypt (Decryption Transform for XML Signature), 10
- Decrypting
 - data, 408–410
 - keys, 412
 - symmetric keys, 414–420
- Decryption
 - cipher text, 410–411
 - Decryption Transform, 376–379
 - in different environment, 179–180
 - key for, 355–356
 - obtaining keying material, 357–358
 - post-decryption processing, 368
 - pre-decryption processing, 367
 - processing, 367
 - processing flow, 365–368
- Decryption Transform, 376–379
- Decryption Transform algorithm, 394
- Default
 - attributes, 184
 - language, 48–49
 - white space, 50
- Default attribute, 93
- #DEFAULT value, 83
- Dereferencing URIs, 240–243
- DES (Data Encryption Standard), 18
 - See also* Triple DES.
- Descendant, 74
- descendant:: axis, 109, 137
- descendant-or-self:: axis, 109, 137
- Detached encryption, 344
- Detached signatures, 209–210
- Detail element, 153
- Detail entries, 153
- DHKeyValue element, 301, 305–306, 308
- Diffie-Hellman algorithm, 387
- Diffie-Hellman Key Agreement algorithms, 401–404
- Diffie-Hellman public key, 305–306
- Digest algorithm, identifying, 222–223
- Digest of data, 214–215
- DigestAlg algorithm, 403, 404
- DigestMethod algorithm, 213
- DigestMethod element, 222–223, 239, 246, 248, 307, 374, 386–389, 395, 397, 403, 414
 - Algorithm attribute, 413
 - P3P (Platform for Privacy Preferences), 258
- DigestValue element, 223, 239, 246, 248, 307, 374, 396–397, 428
- Digital signatures, 17, 21–22, 207
 - algorithms, 213–214
 - appropriate verification key, 225
 - binary signature value, 224–225
 - calculation of, 171
 - canonicalization, 29, 171–178, 249
 - combining with encryption, 371–379
 - converting to sequence of octets, 216–219
 - criticality flag, 229–230
 - cryptographic parts, 228–230
 - data, 214–215
 - enveloped encryption, 27
 - failure, 172
 - generating, 246
 - generation key, 207–211
 - information presented to user, 250–251
 - insecurity of, 172
 - inside encryption, 29
 - meaning, 208
 - message digests, 21
 - messages, 21
 - multiple, 227
 - on only what is seen, 250–251
 - only what is signed is secure, 249
 - outside encryption, 28–29
 - Reference elements, 220–224
 - relevant information, 228–230
 - robust, 29
 - secure, 29
 - security, 248–252

- signature attributes, 229
- SignatureValue element, 224–225
- SignedInfo element, 215–220
- signing encrypted data, 375
- SOAP Envelope, 261–262
- strength of, 251–252
- stringent canonicalization requirements, 130
- syntax, 211–230
- transforms, 248–251
- URI representation, 214
- validation, 264
- verification key, 207–211
- verifying, 216–220, 246–248, 247
- Display agent, 39
- Distinguished name encoding, 311–312
- div operator, 116
- Do nothing canonicalization, 218
- DOCTYPE declaration, 63
- <!DOCTYPE> tag, 71, 72
- Document encoding, 185
- Document entity, 60
- Document order, 101, 139, 193
- Document Style Semantics and Specification Language, 65
- Document-oriented digital signature signature, 232–233
- Documents, 4, 36
 - See also* XML documents
 - appearance of, 63–67
 - describing structure, 70
 - element containing all other elements, 42
 - encoding, 185
 - information about content, 71
 - labels for content, 84–85
 - nesting elements, 42
 - quotes surrounding attribute values, 42
 - root element, 70, 102
 - root element name, 72
 - selecting subsets, 193
 - usable without DTD, 81
 - well-formed, 40–42
 - white space, 49
 - white space outside, 185
- DOM (Document Object Model), 104
- DOM data model, 191
- Domain names, 125
- DOMHASH, 191
- Done Information, 442
- Double apostrophe/double-quote ("), 53, 187
- Draft Standard, 461
- DSA algorithms, 406–407
- DSA (Digital Signature Algorithm) keys, 302–303
- DSA signature algorithm, 302–303
- DSA signatures, 300
- DSAKeyValue element, 213, 301–303, 308
- DSAWithSHA1 algorithm, 392
- ds:CryptoBinary simple type, 213
- ds:KeyInfo element, 348, 354–355, 357–358, 366
- ds:KeyName element, 354, 357, 363–364, 366
- ds:KeyRetrievalMethod element, 363
- ds:KeyValue element, 357
- ds:Reference element, 278, 352
- ds:RetrievalMethod element, 354, 355–356, 358, 363, 366
- DSTC (Distributed Systems Technology Centre), 443
- DSTC Web site, 442–443
- DSTC XMLDSIG product Web site, 443
- ds:Type attribute, 278
- .dtd extension, 71
- DTDNotSupported faults, 153
- DTDs (Document Type Definitions), 6, 39, 42, 44–45
 - basics, 70–71
 - conditional sections, 73
 - data types, 213
 - declaring general entities, 61
 - defining attributes, 79–82
 - element type declarations, 73–79
 - entity reference declarations, 82–84
 - enumerated attribute type, 81–82
 - external, 71–73
 - format, 72
 - general entity references, 83
 - grouping elements, 74
 - guidelines, 73
 - importance in data exchange, 69
 - importance of, 88
 - internal, 71–72
 - KeyInfo element, 297
 - markup declarations, 71
 - name of entity declared in, 80
 - notation declarations, 84–85
 - ordering child elements, 74
 - parameter entities, 62, 83

- DTDs (*cont.*)
 - parameter entity reference declarations, 84
 - signing, 69
 - xml:lang attribute, 48
 - SOAP messages, 147
 - XPath, 102
- E**
- Element content, 299
- Element nodes, 103–104, 195–196
- Element type declarations, 70, 73–79
- Element wrapping, 227
- elementFormDefault attribute, 95
- Elements, 45–47
 - abstract, 96
 - Algorithm attribute, 383
 - ancestor, 74
 - ANY content model, 75
 - any valid character data, 76–77
 - attributes, 47–48, 79–82
 - change of context, 177–178
 - changing enveloping context, 176
 - containers as, 136
 - content, 46, 73–74
 - with content, 45
 - content models, 74–77
 - default attributes, 184
 - descendant, 74
 - empty, 76, 97, 186
 - EMPTY content model, 76
 - end tags, 45
 - frequency indicators, 77–78
 - grouping, 74, 77–78, 94
 - hierarchy, 74
 - ID of another, 80
 - labeling, 81
 - #PCDATA content model, 76–77
 - local, 91
 - locating, 135
 - mixed content, 75, 76–77
 - multiple attributes, 82
 - multiple elements within, 77
 - namespace nodes ordered alphabetically, 194
 - with notation attribute, 84
 - parent-child relationship, 74
 - problems with reenveloping, 176
 - qualified names, 56, 58
 - relationships, 46, 74
 - retaining comments while selecting, 242
 - schemas, 91–95
 - simple naming rules, 46, 47
 - simpleType, 89
 - specifications, 96
 - start tags, 45
 - structures, 74
 - substituting, 97
 - syntax, 73
 - syntax for algorithm-specifying, 384
 - types, 91
 - unique ID, 80, 118
 - unique values, 97
 - values, 93
 - XAdES signatures, 273–274
 - xml:space attribute, 49–50
- EME-OAEP-ENCODE function, 414
- EME-PKCS1-v1_5 function, 412
- EMPTY content model, 76
- Empty elements, 45, 76, 97, 186
- EMSA-PKCS1-V1_5-ENCODE function, 407
- EncapsulatedCRLValue element, 289
- EncapsulatedOCSPValue element, 289
- EncapsulatedPKIValueType data type, 272
- Encoded value of digest output, 223
- Encoding, 52–53
- Encoding attribute, 45
- Encoding declaration, 45
- encodingStyle attribute, 153, 159
- EncryptedData element, 295, 343–344, 346, 350, 352–354, 356–358, 361–362, 364, 367–368, 372, 375, 377–378, 399, 408, 410, 412
- EncryptedKey element, 295–296, 298, 306, 316–317, 343, 350, 354–358, 366–368, 379, 400, 412, 414
 - CarriedKeyName attribute, 308
 - information concerning generation, 352
 - referenced, 363–364
- EncryptedKey elements, 362
- EncryptedType type, 347–349
- Encrypting
 - arbitrary data, 344, 361–362
 - data, 408–410
 - keys, 412
 - symmetric keys, 414–420
 - XML element content, 360–361
 - XML elements, 359
 - XML in place, 344

- Encryption, 9, 477
 - Canonical XML and, 178–180
 - canonicalization, 29, 421
 - care with algorithms and expressions, 369
 - cipher text, 410–411
 - combining with digital signatures, 371–379
 - decryption in different environment, 179–180
 - detached, 344
 - encrypted data, 353
 - enveloping, 344
 - examples, 358–364
 - identifying referent's type, 354–356
 - information revealed, 369
 - as new document root, 353
 - paper point of view, 478
 - plain text before, 348
 - post-encryption processing, 366–367
 - pre-encryption processing, 365
 - private keys, 299
 - processing, 365–366
 - processing flow, 365–368
 - protocol point of view, 478
 - referencing, 344
 - security considerations, 368–369
 - of signed data and signature, 372–373
 - of signed data but not signature, 374
 - signing encrypted data, 375
 - super-encryption, 362–363
 - transporting encryption keys, 354–356
 - triple DES, 409
 - user-readable name with key value, 354–355
 - XML, 368
- Encryption algorithm, 348–349
- Encryption key
 - information about, 348
 - pointers to data and keys encrypted, 354
 - pointers to items encrypted by, 356–357
 - recipient, 355
 - transporting, 354–356
 - type, 355
- EncryptionAlg algorithm, 403
- EncryptionMethod algorithm, 214, 364
- EncryptionMethod algorithm role, 389
- EncryptionMethod element, 348–349, 367, 386, 395, 399, 408, 410–412, 414–415
- EncryptionProperties element, 348, 352–353
- End tags, 45, 82
- end-point() function, 140–141
- Entities, 43, 60–62, 82
 - declaring in DTD, 80
 - values of, 69
- ENTITIES attributes, 80
- ENTITIES type, 204
- ENTITY attributes, 80
- <!ENTITY> declaration, 83
- Entity declaration, 70
- ENTITY declarations, 212
- Entity reference declarations, 82–84
- Entity references, 61, 63, 182–183
- ENTITY type, 204
- Entrust Web site, 443
- Entrust/Toolkit for Java Web site, 443
- Enumerated attribute type, 81–82
- ENUMERATED attributes, 80
- env namespace prefix, 164
- env:DataEncodingUnknown Fault, 164
- Envelope element, 155–158
- Enveloped encryption, 18, 20, 27–29, 306
- Enveloped Signature algorithm, 394
- Enveloped Signature Transform algorithms, 430
- Enveloped signatures, 209–210
- EnvelopedSignature transform, 427
- Enveloping encryption, 344
- Enveloping signatures, 209–210
- env:Server Fault, 164
- equality (=) Boolean operator, 115
- Escaped characters, 80
- ETSI (European Telecommunications Standards Institute), 263–264
- Except element, 377
- Exclusive XML Canonicalization, 169–170, 171, 178, 205, 421
 - comments, 230
 - explicit interoperability testing, 437
 - input/read rules, 182–184
 - namespace nodes output, 198
 - namespace prefixes treated inclusively, 190
 - output namespace declarations, 189–190
 - output/print rules, 184–188
 - serializing attributes, 188
- Exclusive XML Canonicalization algorithms, 218, 388, 423
- Exclusive XML Canonicalization interoperability matrix Web site, 438
- Exclusive XML Canonicalization interoperability page, 442

- Exclusive XML Canonicalization test vectors
 - Web site, 445
 - Exclusive XML Canonicalization with
 - Comments algorithm, 388
 - Explicit transforms, 243
 - Expressions, 112–113
 - context size, 118
 - encryption, 369
 - functions, 114–115
 - operators, 115–117
 - XPointer, 134
 - Extensibility of processing, 474
 - External DTDs (Document Type Definitions), 42, 45, 71–73
 - External entities, 61–62
- F**
- false() function, 121
 - Fault element, 152–155
 - Fault schemas, 155–158
 - faultactor element, 152–153
 - faultcode element, 153
 - faultstring element, 152
 - FIPS (Federal Information Processing Standards), 465, 466–467
 - FIPS home page, 466
 - Firewalls and HTTP (Hypertext Transfer Protocol) binding, 161
 - Fixed attribute, 93
 - #FIXED value, 83
 - floor() function, 122
 - following:: axis, 109
 - following-sibling:: axis, 109, 137
 - Forward axis, 112
 - Frequency indicators, 77–78
 - Fujitsu Web site, 443–444
 - Fujitsu XMLDSIG products Web site, 444
 - Full XPointer, 133–134
 - Function library for XPath, 117–122
 - Functions, 114–115
 - XPointer, 140–143
- G**
- GapXse Web site, 444
 - General entities, 61–62, 82–83
 - Generic URIs (Uniform Resource Identifiers), 124
 - Geuer-Pollmann, Christian, 439
 - GI (generic identifier), 45
- Global attributes, 92, 147
 - Global elements, 91
 - Greater than (>)
 - See also* Right angle bracket.
 - Grouping elements, 77–78
 - Groups, complicated restrictions, 97
 - > > escape string, 53
- H**
- HashDataInfos element, 273
 - Header blocks, 154
 - Header element, 151
 - here() function, 141, 428, 429
 - Hexadecimal character references, 53
 - Historic standard, 461
 - HMAC algorithm, 404
 - HMAC SHA-1 algorithm, 392, 405
 - HMAC variations of algorithms, 406
 - HMAC-MD5 algorithm, 392
 - HMACOutputLength element, 405
 - HMAC-RIPEMD160 algorithm, 392
 - HMAC-SHA256 algorithm, 392
 - HMAC-SHA384 algorithm, 392
 - HMAC-SHA512 algorithm, 392
 - Horizontal tab (xO9) appending space character, 183
 - Hosts and authorities, 124
 - HP Web Services Platform 2.0 Web site, 444
 - HP Web Services Web site, 444
 - href attribute, 147
 - HTML (Hypertext Markup Language), 3–5
 - HTML documents compared with XML documents, 37
 - HTTP (Hypertext Transfer Protocol), 160–162
 - <http://www.w3.org/2000/09/xmlsig#> namespace, 213
 - <http://www.w3.org/2001/12/soap-encoding> encoding, 159
 - Hughes, Merlin, 439, 442
- I**
- IAB (Internet Architecture Board), 459
 - IAIK (Institute for Applied Information Processing and Communications) Web site, 445
 - IANA (Internet Assigned Numbers Authority), 49
 - IBM security suite Web site, 446

- IBM Web site, 445–450
- ID attribute, 80, 81
- id attribute, 147
- ID simpleType, 89
- id() function, 117, 118, 204
- IDREF attributes, 80
- IDREF simpleType, 89
- IDREFS attributes, 80
- IESG (Internet Engineering Steering Group), 459
- IETF (Internet Engineering Task Force), 10, 25, 459–460
- IETF protocols, 479
- IETF tags, 49
- IGNORE keyword, 73
- #IMPLIED value, 83
- in-band key distribution, 316–317
- INCLUDE keyword, 73
- Independent parallel signatures, 278
- Index, 136
- Inequality (!=) Boolean operator, 115
- Infomosaic Web site, 446
- Information, describing structure, 88
- Inherited attribute and namespace declaration rules, 188–190
- INRIA (Institut National de Recherche en Informatique et Automatique), 453
- Integer simpleType, 89
- Integers, 213
- Intermediate-level certification authority, 25
- Internal DTDs (Document Type Definitions), 71–72
- Internal entities, 61–62
- Internal General Entity Reference Declarations, 83
- Internet Explorer semantic attacks, 126
- Internet protocols, 125
- Internet RFC 1766, 36
- Internet Standard, 461
- IOTP, 191
- IPSEC (IP Security), 9, 334
- IPv4 (Internet Protocol), 125
- IPv6, 125
- ISO 639, 36
- ISO 3166, 36
- ISO 10646, 52
- ISO characters, 52
- ISOC (Internet Society), 459
- IssuerTrust aspect string, 329
- IV (initialization vector), 409
- IXSIL (IAIK XML Signature Library), 445
- J**
- Java implementation of XMLDSIG Web site, 446
- Java XKMS reference implementation Web site, 443
- Java-based XML processor, 40
- JDSS II, 446
- K**
- KA-Nonce element, 399, 403
- Karlinger, Gregor, 439, 445
- Keio University of Japan (Shonan Fujisawa Campus), 453
- Kerberos, 18
- Key agreement algorithms, 398–404
- Key binding
 - information associated with, 325
 - registered by service, 334
 - registration, 331
 - status, 328
 - XML digital signature, 337
- Key Information Services, 319, 321–327
- Key pair, clients or servers generating, 332
- Key recovery, 331
- Key registration messages, 331–334
- Key Registration Service, 319
- Key revocation, 331
- Key rollover, 30–31
- Key transport algorithms, 412–414
- Key wrapping, 416–420
- KeyBinding element, 331, 333–336
- KeyBindingAuth element, 336, 337
- Keyed hash authentication codes, 251
- KeyID, 324
- KeyInfo element, 225, 247, 275, 293, 295, 310, 344, 367, 387, 399–400, 412, 414
 - child elements, 295, 297–299
 - DTDs (Document Type Definitions), 297
 - information stored at another location, 306–308
 - namespace prefixes, 296
 - schema notation, 296
 - syntax, 296–297
- KeyInfo formats, 259
- KeyInfo type element algorithm, 214
- KeyName element, 298, 308–309, 311, 367

- KeyName string, 330
- KeyReference elements, 357, 358
- Keys
 - algorithm invocation, 308
 - certificates containing validation key, 310
 - client authorized to register, 336
 - decrypting, 412
 - elements desired in response, 329
 - encrypted by another key, 306
 - encrypting, 412
 - helping recipient choose, 309–314
 - identifying to recipient, 308–309
 - information concerning, 322
 - KeyID, 324
 - PGP public key pairs and signatures, 314–315
 - randomness, 29–30
 - registration of server generated, 337–338
 - registration of user-generated, 336–337
 - result codes, 328
 - results of validation, 327
 - shared secret data, 335–336
 - status of assertion, 328
 - types of usage, 325
 - URI identifier, 324–325
 - valid or indeterminate status, 328–329
 - validity, 322
- KeySize element, 349, 399, 403
- KeyValue element, 298
- KeyValue string, 330
- L**
 - lang() function, 121
 - Language, default, 48–49
 - Language tags, 121
 - last() function, 118
 - #PCDATA content model, 76–77
 - Left angle bracket (<), 42, 52–53, 63, 187
 - Legal characters, 52
 - Less than (<), 42, 52–53, 63, 187
 - Line breaks, 182–183
 - Line separator character, 44
 - List types, 97
 - Literal prefix names, 100
 - Local attributes, 92–93
 - Local elements, 91
 - local-name() function, 118
 - Locate Service, 322–324
 - Location paths, 107–112
 - Location points, 140–141
 - Location steps
 - axis, 108, 109–110
 - node tests, 108, 110
 - predicates, 108, 110–112
 - Locations, 135–136, 140, 142
 - Location-sets, 135–136, 140
 - selecting points from, 137
 - with single member, 141
 - string value of items, 142–143
 - Logical assertion markup, 38
 - Logical structure, 43
 - attributes, 47–48
 - CDATA sections, 50–51
 - character sets, 52–53
 - comments, 51–52
 - elements, 45–47
 - encoding, 52–53
 - PIs (processing instructions), 54–55
 - special attributes, 48–50
 - XML declarations, 44–45
 - Lower-level certification authorities, 24
 - < < escape string, 53
- M**
 - MAC (Message Authentication Code)
 - algorithms, 404–406
 - MAC (hash) function output value, 325
 - Machine validation of document structure, 88
 - MACs (message authentication codes), 15–17
 - mailto: scheme, 127
 - Manifest element, 221, 227–228, 245–246, 376
 - Markup, 4, 43
 - Markup declarations, 70–71
 - Markup languages, 35
 - Markup tags, creation of, 6–7
 - MD5 algorithms, 390, 395–397
 - Message digest algorithms, 29, 385, 395–398
 - Message digests, 13–15, 21
 - Messages
 - converting to fixed-length binary fingerprints, 13
 - digital signatures, 21
 - MGF1 function, 414
 - MgmtData element, 298, 316–317
 - MgmtData string, 330
 - Microsoft Web site, 447
 - Middle attribute, 93
 - MIME type of encrypted data, 348

- Minimal Canonicalization, 172, 218, 423–424
- Minimal Canonicalization algorithms, 388, 423–424
- Misunderstood element, 154
- MIT/LCS (Massachusetts Institute of Technology's Laboratory for Computer Science), 453
- mod operator, 116
- Moving resources, 128
- Multiple string, 330
- mustUnderstand attribute, 148, 150–151, 154
- MustUnderstand fault, 147–148, 152–155

- N**
- Name attribute, 91
- Name tokens, 81
- name() function, 118, 190
- Names
 - colon (:) in, 57
 - prohibiting from starting with numbers, 47
- Names entities content, 63
- namespace:: axis, 109, 137
- Namespace attribute, 94–95, 96
- Namespace identifier, 147
- Namespace nodes, 104–105
 - canonicalization, 197–198
 - covering range, 138
- Namespaced references to profiles, 175
- Namespace-qualified name, 153
- Namespaces, 55
 - algorithm-specific, 383
 - allowable, 94–95
 - alphabetic order, 194
 - binding, 200
 - classes of namespaces, 94
 - colon (:) reserved for, 47
 - declaration inheritance, 188–190
 - declarations, 57–58
 - explicitly matching prefix names, 175
 - guidelines, 59
 - inclusion/exclusion of ancestor declarations, 205–206
 - inputting components from other, 96
 - local elements and attributes, 95
 - ordering, 186
 - prefix declaration affecting all child nodes, 174–175
 - prefixes, 56, 58–59
 - problems with, 174–178
 - qualified names, 58
 - qualifying all global elements and attributes, 95
 - relative URIs, 205
 - schemas, 89, 95–96
 - SOAP, 147
 - superfluous declaration deletion, 188–190
 - uniqueness, 57
 - URIs (Uniform Resource Identifiers), 59
 - XML, 37
- namespace-uri() function, 119
- NBS (National Bureau of Standards), 465
- ::NCName:* node test, 111
- NDATA keyword, 62
- NEC Web site, 447–448
- Netscape Navigator
 - random number generator for SSL keys, 30
 - semantic attacks, 126
- New line (`xOA`) appending space character, 182–183
- Nilable elements, 97
- NIST (U.S. National Institute of Science and Technology), 465–466
- NMTOKEN attributes, 80–81
- NMTOKENS attribute, 81
- NMTOKENS simpleType, 89
- Node test (::*), 111
- Node tests, 108, 110, 138
- ::node() node test, 111
- Node-point, 136, 139
- Nodes, 140
 - actors, 150
 - covering range, 138–139
 - document order, 101, 139
 - name with namespace prefix, 190
 - number in parameter, 117
- Node-sets, 107, 140, 190, 192, 378–379, 426
 - document order, 193
 - functions, 117–119
 - operators, 115
 - same-document URI references, 241
 - union of, 115
 - unordered, 193
 - XML canonicalization, 241–242
- Non-cryptographic algorithms, 421–433
- none actor, 150
- Non-null URIs, 242–243
- Nonvalidating parser/processors, 39–40
- normalize-space() function, 119

- NOTATION attribute, 81
- NOTATION declarations, 54, 204
- Notation declarations, 70, 84–85
- Notations
 - canonicalization, 204
 - names of, 81, 84
 - problems with canonicalization, 85
- Note, 454
- not() function, 121
- Null URIs, 242
- Number element, 361
- Number functions, 122
- number() function, 114, 122
- Numeric character references, 53
- Numeric IPv6 addresses, 125

- O**
- OAEP (Optimal Asymmetric Encryption Padding), 413
- OAEP encryption algorithms, 385
- OAEPparams element, 413, 414
- OASIS (Organization for the Advancement of Structured Information Standards) consortium, 11
- Object element, 225–227, 265
- ObjectIdentifierType data type, 271–272
- ObjectReference attribute, 279
- Objects, converting to strings, 120
- OCSP (Online Certificate Status Protocols), 26–27, 285
- OCSP string, 330
- OCSP (Online Certificate Status Protocol) tokens, 314
- OCSPValues (OCSP Responses), 289–290
- Octothorpe (#), 129
- OIDs (object identifiers), 271
- Opera browser and semantic attacks, 126
- Operational nonequivalence, 203–204
- Operators, 115–117
- Or Boolean operator, 115
- origin() function, 141
- OSI X.500 Directory standard, 25
- Output/print rules, 184–188
- Overall system security, 32

- P**
- p (prefix) entity, 212
- P3P (Platform for Personal Privacy Protection), 453
- P3P (Platform for Privacy Preferences), 253
 - Assures element, 254–256
 - CanonicalizationMethod, 258
 - DigestMethod, 258
 - KeyInfo formats, 259
 - limitations, 258–259
 - SignatureMethod algorithms, 258
 - transforms, 259
 - XMLDSIG links to semantics, 254–255
 - XMLDSIG use, 257–258
- P3P policy, 254
- Padding algorithm, 409
- Padding method, 385
- Paper point of view, 469–470, 480
 - adjunct meaning, 472
 - amount of processing, 473
 - authentication, 476
 - canonicalization, 475
 - core meaning, 471
 - encryption, 478
 - extensibility of processing, 474
 - granularity of processing, 473
 - unique internal labels, 478
- Parameter entities, 61–62, 83
- Parameter entity reference declarations, 84
- Parameter node-set, 118–119
- Parameters, 117, 121
- parent:: axis, 110, 137
- Parent element, 45
- Parsed data, 43
- Parser/processors
 - information about document content, 71
 - nonvalidating, 39–40
 - protecting information from, 50
 - UTF-8, 45
 - UTF-16, 45
 - validating, 39–40
 - XML, 45
- Pass phrase, 335
- PassPhraseAuth element, 336, 337
- Patents, 11
- Paths and URIs (Uniform Resource Identifiers), 126–127
- Payment element, 359
- PCDATA, 50
- Percent sign (%), 129
- Personnel security, 31, 32
- PGP (Pretty Good Privacy), 9, 25

- PGP public key identifier, 314
- PGP string, 330
- PGPData element, 298, 314–315
- PGPKeyID element, 314
- PGPKeyPacket element, 314
- PGPWeb string, 330
- Phaos for XMLDSIG, XML Canonicalization, and XML Encryption Web site, 448
- Phaos Technology Web site, 448
- Physical randomness, 30
- Physical security, 31, 32
- Physical structure, 60–63
- PICS (Platform or Internet Content Selection), 453
- PIs (processing instructions), 54–55
- PKCS #7 signedData structure, 313–314
- PKCS7signedData element, 308, 310, 313–314
- PKCS#1 specification, 406
- Plain text, 17
- Plain text, limited-use, shared secret pass phrase, 335
- Plain text types, 349
- Point location extension:, 136–137
- Point type, 136–137
- Pointers, 127
- Points
 - covering range, 138
 - document order, 139
 - index, 136
 - for locations, 142
 - preceding node, 139
- Point-to-point security, 9
- position() function, 119
- Post-decryption processing, 368
- Post-encryption processing, 366–367
- Pound sign (#)
 - See also* Octothorpe
- Pouliot, Sebastien, 448
- Poupou, 448
- preceding:: axis, 110
- Preceding node, 139
- preceding-sibling:: axis, 110, 137
- Pre-decryption processing, 367
- Predefined entity references, 42
- Pre-defined simpleType construct, 89
- Predicates, 108, 110–112
- Pre-encryption processing, 365
- Prefixes, reserved, 58
- Privacy policies, 254–259
- Private element, 334
- Private key element, 329
- Private keys, 251
 - compromised, 25–26
 - encryption, 299
 - parameters generated by registration service, 334
 - process to release to, 331
 - XML digital signatures, 299
- Private string, 330
- Procedural security, 31
- processContents attribute, 94
- Processing instruction nodes, 106, 199
- Processing Instructions and SOAP messages, 146
- ::processing-instruction (Literal) node test, 111
- Prolog, 37, 70
- ProofOfPossession element, 336, 337
- Proposed Recommendations, 454, 455
- Proposed Standard, 461
- Protocol point of view, 469–470, 480
 - adjunct meaning, 472–473
 - amount of processing, 473
 - authentication, 476–477
 - canonicalization, 475–476
 - core meaning, 472
 - encryption, 478
 - extensibility of processing, 474
 - granularity of processing, 473–474
 - unique internal labels, 478–479
- Public identifier, 62
- Public key algorithms, 21
- Public key authentication and digital signatures, 21–22
- Public key ciphers, 19–20
- Public key encryption systems, 27
- Public key infrastructure, 331
- Public key signature algorithm, 385
- Public keys, 251, 331
 - authenticating, 335–336
 - binding between data elements, 325–326
 - certificates, 23
 - queries, 322–323
 - rollover, 30–31
 - root, 23
 - secret quantity shared between sender and recipient, 398

- Public keys (*cont.*)
 - top-level, 23
 - value of, 299–306
- Public/private key pair, 332
- Q**
 - qname attribute, 154
 - ::QName node test, 111
 - Qualified names, 58
 - Queries and public key, 322–323
- R**
 - Radioactive decay, 30
 - Random number generation, 30
 - Randomness, 29–30
 - Range location extension, 137–138
 - range() function, 141
 - range-inside() function, 141
 - Ranges, 137–139, 141
 - range-to() function, 142
 - RC4 algorithm, 411
 - Reagle, Joseph, 450
 - Receiver faults, 153
 - RecipientKeyInfo element, 398
 - Recommendations, 454
 - Ref attribute, 91, 94
 - Reference element, 214, 220–224, 245–246,
 - 260, 297, 299, 307, 374, 376, 393, 396, 424
 - dereferencing URIs, 240–243
 - validating, 246
 - ReferenceList element, 351, 354, 356–357, 364
 - References
 - generation, 245–246
 - same-document, 241–242
 - verification, 247–248
 - Referencing encryption, 344
 - Register element, 332–333
 - Relative location paths, 107
 - Relative URIs (Uniform Resource Identifiers),
 - 127–128, 130
 - base URI for, 131–132
 - canonicalization, 204
 - as namespaces, 205
 - Request message, 326–327, 332–333
 - #REQUIRED value, 83
 - Required-SOAPAction HTTP Header, 162
 - Reserved prefixes, 58
 - Resource-constrained applications, 217
 - Resources, 128
 - Respond element, 333
 - Response message, 327, 333–334
 - Restricting content, 94–95
 - Result tree, 65–66
 - RetrievalMethod element, 297–299, 306–308,
 - 367, 386, 393, 424
 - RetrievalMethod string, 330
 - Reverse axis, 112
 - RevocationValues element, 289–290, 291
 - RFC Editor Web site, 462
 - RFCs (Requests for Comments), 459
 - access to, 461–462
 - ASCII format, 462–463
 - BCP (Best Current Practice) standard, 461
 - Draft Standard, 461
 - Experimental status, 460
 - format to, 462–463
 - Historic standard, 461
 - Informational status, 460
 - Internet Standard, 461
 - Proposed Standard, 461
 - Right angle bracket (>), 52–53
 - Rijndael, 18
 - RIPEMD-160, 389
 - RIPEMD-160 algorithms, 390, 398
 - Root elements, 45, 75, 102
 - Root node, 101–103
 - canonicalization, 195
 - containers as, 136
 - covering range, 138
 - multiple child elements, 136
 - processing child nodes in document order,
 - 195
 - Root public keys, 23
 - round() function, 122
 - rpc namespace prefix, 164
 - rpc:BadArguments Fault, 164
 - rpc:ProcedureNotPresent Fault, 164
 - RPCs (Remote Procedure Calls)
 - Faults, 164
 - information required, 163
 - schemas, 164
 - SOAP, 162–166
 - RSA (Rivest-Shamir-Adelman) algorithm, 304
 - RSA key pairs, 338
 - RSA keys, 304
 - RSA Security Web site, 449
 - RSA signatures, 300
 - RSA variations of algorithms, 408

- RSA Version 1.5 algorithms, 412–413
 - RSAES-PKCS1-v1_5 algorithm, 412
 - RSAKeyValue element, 301, 304, 308
 - RSAKeyValue value, 213
 - RSA-OAEP, 413
 - RSA-OAEP algorithms, 391, 413–414
 - RSA-SHA1 algorithms, 407–408
 - RSASSA-PKCS1-v1_5 encoding/padding algorithm, 407
 - RSA-v1.5 algorithm, 391
 - RSAwithMD5 algorithm, 392
 - RSAwithRIPEMD160 algorithm, 392
 - RSAwithSHA1 algorithm, 392
 - RSAwithSHA256 algorithm, 392
 - RSAwithSHA384 algorithm, 392
 - RSAwithSHA512 algorithm, 392
- S**
- s (suffix) entity, 212
 - Salz, Richard, 450
 - Same-document references, 241
 - Same-document XPointers, 242
 - SAML (Security Assertion Markup Language), 11
 - Sanin, Aleksey, 451
 - Schema algorithm, 394
 - Schema element, 89
 - Schema validation transform, 432
 - schemaLocation attribute, 96
 - Schemas, 39, 69, 87
 - abstractness, 96
 - advantages, 87
 - annotations, 96
 - anyType type, 94
 - construct, 90
 - content from different files, 95
 - data types, 213
 - default attribute, 93
 - disadvantages, 87–88
 - elements and attributes, 91–95
 - fault, 155–158
 - fixed attribute, 93
 - global attributes, 92
 - instance of, 88
 - in instances, 97
 - local attributes, 92–93
 - namespaces, 89, 95–96
 - overview, 88–89
 - RPCs (Remote Procedure Calls), 164
 - simpleType construct, 89–90
 - types, 89–90
 - validation, 432–438
 - Schemes and registry, 124
 - Secret key ciphers, 17
 - Secret key in MACs (message authentication codes), 15
 - Secure symmetric authentication algorithms, 371
 - Secure symmetric encryption algorithms, 371
 - Secure Telnet, 31–32
 - Secure XML Verify() Web service Web site, 446
 - Security, 6
 - actively monitoring for intrusion or compromise, 32
 - authentication, 8
 - confidentiality, 9
 - cryptographic algorithms or formats, 32
 - difficulty of forging signatures, 251–252
 - encryption, 9, 368–369
 - key rollover, 30–31
 - non-XML mechanisms, 9
 - by obscurity, 32
 - overall system, 32
 - personnel, 31, 32
 - physical, 31, 32
 - point-to-point, 9
 - procedural, 31
 - proper canonicalization, 32
 - randomness generation, 32
 - secrecy of symmetric and private keys, 32
 - signatures, 248–252
 - stylesheets, 64
 - Security HMAC, 15
 - self:: axis, 110, 112, 137
 - Sender faults, 153
 - Sequence of octets, 190
 - Server-generated keys, registration, 337–338
 - Servers
 - generating key pair, 332
 - trusted relationship with, 319
 - SGML (Standard Generalized Markup Language), 3, 35
 - SGML Editorial Review Board, 4
 - SHA versions of algorithms, 397–398
 - SHA-1 algorithms, 390, 397
 - SHA-256 algorithm, 390, 397
 - SHA384, 389
 - SHA-384 algorithm, 390, 397

- SHA512, 389
- SHA-512 algorithm, 390, 397
- Shared secret data, 335–336
- Siggen Web site, 449
- Signature algorithms, 216, 251, 406–408
- Signature applications and Canonicalization-Method algorithms, 217
- Signature aspect string, 329
- Signature element, 215, 227, 245, 351, 372, 374, 379, 387, 399–400, 428, 430
 - algorithms, 213–214
 - detached, 257
 - enclosing policy, 258
 - failure to verify, 247
 - putting data inside, 225–227
 - SOAP, 259
 - steps required to produce and verify, 245–248
 - syntax, 215
- Signature generation, 245–246, 246
- Signature strength, 251–252
- Signature test vectors Web site, 445
- Signature verification, 246–248
- Signature verifier, 22
- SignatureMethod algorithm role, 389
- SignatureMethod algorithms, 213, 216, 227, 258
- SignatureMethod elements, 214, 219–220, 246–247, 395, 399, 405–407
- SignatureMethod role element, 386
- SignaturePolicyIdentifier element, 275–277
- SignatureProperties element, 227, 228–230, 254
- SignatureProperty element, 254
- Signatures, 207
 - binary format in PGP, 208
 - binary format in PKCS#7, 208
 - canonicalization, 421
 - detached, 209–210
 - difficulty in forging, 251–252
 - enveloped, 209–210
 - enveloping, 209–210
 - independent parallel, 278
 - new format for, 208–209
 - security, 248–252
 - XML syntax, 208–209
- SignatureTimestamp element, 284, 291
- SignatureValue element, 214, 224–225, 247, 405–408, 428
- SignedDataObjectProperties element, 268, 269–270
- SignedInfo element, 214–220, 246–248, 295, 376, 387
- SignedProperties element, 265, 268
- SignedSignatureProperties element, 268, 269
- SignedSignatureProperty element, 279, 281
- SignerContactInfo element, 281–282
- SignerRole element, 282–283
- Signing encrypted data, 375
- SigningCertificate element, 274–275
- SigningTime element, 274
- SigPolicyID element, 276
- SigPolicyQualifier element, 276
- Simple protocol digital signature example, 230–232
- Simple XML, 55
- simpleType construct, 89–90
- SimpleTypes, 89
- Single apostrophe/single-quote ('), 53
- Single-Request-Response TMEP, 160
- Skeletal XML, xxi
- S/MIME (Secure Multipurpose Internet Mail Extensions), 9
- SML compatibility with SGML, 6
- SMTP default port number, 160
- SOAP, 145, 253
 - application signature profile rules and recommendations, 260–261
 - application/soap MIME type, 162
 - attributes, 149
 - basics, 145–147
 - Blocks, 150
 - Body Block, 163
 - Canonicalization, 260
 - encoding, 158–159
 - encoding schema, 481–494
 - Envelope element, 155–158
 - envelope syntax, 147
 - envelope version change, 154
 - fault schemas, 155–158
 - faults, 152–155
 - features included and excluded, 146
 - global attributes, 147
 - HTTP (Hypertext Transfer Protocol) binding, 161–162
 - HTTP RPCs (Remote Procedure Calls), 163–164
 - <http://www.w3.org/2001/12/soap-encoding> encoding, 159
 - MustUnderstand Fault, 147, 152

- namespace identifier, 147
- namespaces, 147
- nodes, 148
- refinement of, 10
- relation to XML, 146–147
- Required-SOAPAction HTTP Header, 162
- RPCs (Remote Procedure Calls), 162–166
- signature blocks, 260
- Signature element, 259
- single request-response TMEP, 161
- SOAPAction: HTTP Header, 162
- transport message exchange patterns, 160
- Upgrade element, 147
- VersionMismatch Fault, 148, 154
- XKMS, 320, 324
- XMLDSIG, 259–262
- XPath, 261
- SOAP applications and SOAP messages, 260
- SOAP Envelope and digital signatures, 261–262
- SOAP Envelope element, 260
- SOAP messages
 - Body element, 148, 149, 151
 - DTDs (Document Type Definitions), 147
 - elements and attributes are namespace qualified, 146
 - Header Blocks, 152
 - Header element, 148, 149, 151
 - optimizing processing, 162
 - procedure call request, 163
 - Processing Instructions, 146
 - restrictions, 146–147
 - schema processing, 147
 - SOAP applications, 260
 - SOAP Blocks, 150
 - stopping processing, 152
 - transport protocol, 160
 - XML digital signatures, 259
- SOAP nodes, 150, 152
- SOAPAction: HTTP Header, 162
- Soap-envelope namespace, 150
- Sound and XML (Extensible Markup Language), 38
- Sound markup, 38
- Source tree, 65, 66
- Space (`x20`) appending space character, 183
- Special character strings, 52–53
- Special characters, 182–183, 187
- SPKI (Simplified Public Key Infrastructure)
 - certification system, 25
 - SPKI public key pairs, 315–316
 - SPKI string, 330
 - SPKIData element, 298, 315–316
 - SPKISexp element, 315
 - Square brackets ([]), 129
 - SSL (Secure Sockets Layer), 9
 - SSN element, 361
 - Standalone attribute, 45
 - Standalone document declaration, 45
 - Standardized, well-formed HTML, 5
 - Start tags, 45
 - attributes, 47–48, 79
 - empty element tags, 79
 - white space between attributes, 173
 - start-point() function, 142
 - starts-with() function, 119
 - Status aspect string, 329
 - Stream encryption algorithms, 410–411
 - String functions, 119–120
 - string() function, 114, 120
 - string-length() function, 120
 - string-range() function, 142
 - Strings, 89, 119–120
 - Stylesheets, 39, 63
 - CSS (Cascading Style Sheets), 64–65
 - security, 64
 - XSL (Extensible Stylesheet Language), 65–66
 - Subdocuments, 99
 - Subset data, 132
 - substring-after() function, 120
 - substring-before() function, 120
 - substring() function, 120
 - Substrings, 119, 120
 - subtraction (-) operator, 116–117
 - sum() function, 122
 - Super-encryption, 362–363
 - Symmetric cipher, 27
 - Symmetric key ciphers, 17–18
 - Symmetric key wrap algorithms, 414–420
 - Symmetric keys, 414–420
 - Symmetric secret key authentication, 207
 - System identifier, 62
 - SYSTEM keyword, 72, 73

T

 - Tags, 36, 38
 - targetNamespace namespace, 95
 - TCP (Transmission Control Protocol), 126

- Test vectors for XMLDSIG Web site, 450
- Text, 60
 - normalized or standardized, 171
 - white space added to, 174
 - XML documents, 38
- Text canonicalization, 217
- Text nodes, 105–106, 198–199
- Text-based canonicalization algorithms, 217
- Textual objects as well-formed XML
 - document, 40–41
- Thermal noise, 30
- Timestamp Authority, 272–273
- Timestamps, 272–274
- TimeStampType data type, 272–273
- T.J. Mather Web site, 447
- TLS (Transport Layer Security), 9, 334
- TMEP (Transport Message Exchange Pattern)
 - model, 160
- Tokens, 135
 - allowed characters, 44
 - list of, 80
- Top element, 93
- Top-level certification authorities, 23–24
- Top-level public keys, 23
- Transform algorithms, 213–214, 239, 393, 424–433
- Transform element, 377, 386, 421, 424, 430–431
- Transform role in canonicalization algorithms, 387
- Transforms, 222, 245–246
 - automatic, 243–244
 - data pipeline, 243–244
 - digital signatures, 248–251
 - element syntax, 244–245
 - explicit, 243
 - P3P (Platform for Privacy Preferences), 259
 - XPath, 239–245
 - XPath evaluation, 427
 - XPath input, 426
 - XPath output, 426–427
- Transforms element, 222, 351, 357, 367, 393, 424
- translate() function, 120
- Tree transformation, 65–66
- Triple DES, 18
- Triple DES algorithms, 409–410
- Triple DES Key Wrap algorithm, 391, 415–416
- TRIPLEDES algorithm, 391
- true() function, 121
- TSP (Trusted Service Provider), 290
- Type attribute, 91
- Type URIs, 299
- U**
- Unicode, 38
- Unicode and ISO/IEC 10646, 36
- Unicode characters, 43, 129
- Unicode Normalization Form C, 202
- Union types, 97
- Unique internal labels, 478–479
- Unparsed data, 43
- Unparsed entities, 62, 84
- Unparsed external entities, 204
- UnsignedDataObjectProperties element, 268, 271
- UnsignedProperties element, 265–266, 268–269
- UnsignedSignatureProperties element, 267–268, 270
- Upgrade element, 147, 154
- URIs (Uniform Resource Identifiers), 56–57, 123, 245
 - ASCII characters, 128, 129
 - authorities, 124–126
 - base, 130–132
 - dereferencing, 240–243
 - disallowed characters, 129
 - domain names, 125
 - encoding, 128–130
 - encoding rules, 130
 - fragment specifiers, 128
 - host specification, 125
 - hosts, 124
 - most restrictive to most general, 159
 - most specific, 221
 - namespaces, 59
 - non-null, 242–243
 - numeric address, 125
 - other references, 242–243
 - paths, 126–127
 - query component, 127
 - reference ending with fragment specifier, 242
 - references, 128
 - relative, 127–128, 130
 - representation in digital signatures, 214
 - retrieving document or page, 127–128

- same-document references, 241–242
 - schemes, 124
 - sequence of octets, 129
 - styles for algorithms, 385, 387
 - syntax, 124–127
 - Unicode characters, 129
 - XPointers, 132
- URLs (Uniform Resource Locators), 123
- URNs (Uniform Resource Names), 123
- U.S. Digital Signature Algorithm, 303
 - See also* DSA.
- Use attribute, 93
- User-generated keys registration, 336–337
- UTF-8, 45
 - character encoding, 185
 - encoding, 52
- UTF-16, 45
 - character encoding, 185
 - encoding, 52
- V**
- Valid XML documents, 39, 42–43
- Validate element, 326–327
- Validate Service, 322, 324–327
- ValidateResponse message, 327
- Validating parser/processors, 39–40
- ValidityInterval aspect string, 329
- Values, selecting value from, 80
- Variables and entities, 82
- Verification in canonicalization, 29
- Verification key, 247
- Verisign, Inc. X.509v3 certificates, 26
- Verisign Web site, 449–450
- Verisign XKMS Java toolkit/SDK Web site, 449–450
- Verisign XML Signature Java SDK Web site, 449
- VersionMismatch Fault, 148, 153, 154
- Vertical bar character (|), 115
- Video and XML (Extensible Markup Language), 38
- VXML (Voice Extensible Markup Language), 8
- W**
- W3C (World Wide Web Consortium), 4, 453, 460
- W3C Core XML Group, 170
- W3C documents, 454–456
- W3C Schema Recommendation language, 88
- W3C software disclaimer, 456–458
- W3C Web site, 450
- W3C Web site Technical Reports page, 454
- Web pages, 5, 127
- Web sites, standard format for privacy policies, 254–259
- WebSig Web site, 450
- Wedgetail product Web site, 451
- Wedgetail Web site, 450–451
- Well-formed documents, 40–42
- Well-formed XML documents, 39, 71
- White space, 49
 - added inside element, 174
 - added to actual text content, 174
 - between attributes in start tag, 173
 - in content, 187
 - default, 50
 - inside start and end tags, 173, 187
 - outside documents, 185
 - preserving, 82
 - problems, 173–174
 - processing between CDATA and non-CDATA attributes, 184
 - in processing instructions, 187
- White space characters, 183
- Windows machine Character Map, 53
- Working Draft, 454
- World Wide Web interoperable specifications for content, 4
- X**
- X.500 identities, 25
- X.506v3 Certificate standard, 479
- X.509 certificates, 25
- X.509 CRL (certificate revocation list) structure, 26
- X509 distinguished names, 311–312
- X.509 issuer, 309
- X.509 subject distinguished name, 309
- X509 V.3 certificate, 309
- X509 V.3-SubjectKeyIdentifier extension, 309
- X509Cert string, 330
- X509Certificate element, 309
- X509Chain string, 330
- X509CRL element, 310
- X509CRL string, 330
- X509Data element, 275, 298, 309–314
- X509IssuerName element, 311
- X509IssuerSerial element, 275, 309, 310

- X509SKI element, 309, 310
- X509SubjectName element, 309–311
- X.509v3 certificates, 25–26
- X.509v3 mesh certificates, 25
- XACML (eXtensible Access Control Markup Language), 11
- XAdES (XML Advanced Electronic Signature), 10, 264, 265
- XAdES signatures, 263–264
 - accessible validation data, 284–285
 - certificate chain references, 284
 - collecting certificates for, 288–289
 - creation and validation rules, 275–277
 - CRLValues (certificate revocation lists), 289–290
 - data countersigned by appropriate entities, 277–278
 - data types, 271–273
 - elements, 273–274
 - format types, 278–279
 - independent parallel, 278
 - information about signer, 281–282
 - levels, 264
 - OCSPValues (OCSP Responses), 289–290
 - revocation information, 284–287, 289–290
 - securing archival signatures, 290–291
 - SignedProperties element, 268
 - signer's role, 282–283
 - single signed data item format, 278–279
 - source of signer identity, 274–275
 - syntax basics, 268–273
 - timestamp, 274
 - timestamp before signing, 283–284
 - timestamp certificates and revocation information, 287–288
 - timestamp over, 284
 - UnsignedProperties element, 268
 - validation, 284–291
 - what signers have bound themselves to, 279–280
- XAdES (XML Advanced Electronic Signature), 264, 265
- XAdES-A (XAdES-XL with one or more embedded archival time stamps), 264, 268
- XAdES-C (XAdES-T with complete validation data references), 264, 266
- XAdES-T (XAdES with additional time stamp), 264, 266
- XAdES-X (XAdES-C with extended validation data), 264, 267
- XAdES-XL (XAdES-X with complete validation data information), 264, 267
- XAdES-A (XAdES-XL with one or more embedded archival time stamps), 264, 268
- XAdESArchiveTimestamp element, 290–291
- XAdES-C (XAdES-T with complete validation data references), 264, 266
- XAdESCompleteTimeStamp element, 287–288, 291
- XAdESRefOnlyTimeStamp element, 288, 291
- XAdES-T (XAdES with additional time stamp), 264, 266
- XAdES-X (XAdES-C with extended validation data), 264, 267
- XAdES-XL (XAdES-X with complete validation data information), 264, 267
- Xalan package, 438–439
- XBULK, 334
- XHTML (Extensible Hypertext Markup Language) Recommendation, 5
- XInclude (XML Inclusions), Version 1.0, 37
- X-KISS (Key Information Service Specification), 320
 - relieving clients of actions, 321
 - services, 321–327
- XKMS (XML Key Management Specification), 10, 145
 - common data elements, 327–329
 - cryptographic algorithms, 334–338
 - namespace prefixes, 320
 - respond strings, 330
 - SOAP, 320, 324
 - XML Key Management system, 319–320
- XKMS Interoperability Web Service (.NET) Web site, 448
- XKMS Note, 338
- XKMS WG (W3C XKMS working group), 339
- xkms:AssertionStatus element, 328
- xkms:AuthInfo element, 332
- xkms:KeyBinding element, 325–326, 331
- xkms:KeyBinding model, 324
- xkms:KeyBindingAuth element, 335–336
- xkms:KeyId element, 324–325
- xkms:KeyUsage element, 325
- xkms:PassPhrase element, 325
- xkms:PassPhraseAuth element, 335

- xkms:ProcessInfo element, 325
- xkms:Prototype element, 325–326
- xkms:Query element, 325–326
- xkms:Reason element, 328–329
- xkms:Respond element, 322, 329
- xkms:ResultCode element, 324, 328
- xkms:ValidityInterval element, 324
- X-KRSS (Key Registration Service Specification)
 - all-purpose Register operation, 331
 - key recovery, 331
 - key registration messages, 331–334
 - key revocation, 331
 - parameters generated by registration service, 334
 - registration, 331
- XLink (XML Linking Language), Version 1.0, 37
- XML (Extensible Markup Language), xvii, 3, 479
 - 1.0 (second edition), 36
 - advantages and disadvantages, 6–7
 - arbitrary-length integers, 213
 - basics, 35–67
 - canonicalization, 172–173
 - case sensitivity, 41
 - combining encryption with XMLDSIG, 368
 - comments, 230
 - design, 6
 - design goals, 3
 - encryption, 368
 - encryption and Canonical XML, 178–180
 - extensible style sheet, 7
 - failure to canonicalize content, 249
 - flexibility, 7
 - goals, 5–6
 - lack of automated processing libraries, 7
 - mapping application parameter names into, 165–166
 - meaning behind markup, 38
 - namespace problems, 174–178
 - need for security, 8–9
 - origins, 4
 - overview, 3–8
 - parsing process, 39–40
 - pointers, 127
 - processing instructions, 230
 - readable formatting, 173
 - relation of SOAP, 146–147
 - schema context, 212
 - schema validation transform, 432
 - sound, 38
 - stylesheets, 63–67
 - supporting variety of applications, 5
 - syntax for marking up, 38
 - usable over Internet, 5
 - uses of, 8
 - verbosity, 7
 - video, 38
 - white space problems, 173–174
- XML Advanced Electronic Signatures, 263
- XML applications allowed syntax, 69
- XML Base, 37
- XML Canonicalization
 - node-sets, 241–242
 - requires returning original prefix, 190
 - XPath expressions, 242
- XML canonicalization data model, 190–194
- XML declarations, 44–45
- XML Digital Signature applications, 406
- XML Digital Signature Software Library Web site, 448
- XML Digital Signature standard, 246, 383, 397, 405, 422
- XML digital signatures, 334
 - complex form example, 237–239
 - complex protocol example, 234–236
 - examples, 230–239
 - IOTP, 191
 - key binding, 337
 - private keys, 299
 - simple document example, 232–233
 - simple protocol example, 230–232
 - SOAP messages, 259
 - syntax, 211–230
- XML documents, 36
 - See also* documents
 - accessing content and structure, 39–40
 - body, 37, 70
 - comments, 51–52
 - compared with HTML documents, 37–38
 - compatibility between, 6
 - DTD, 42
 - ease of creation, 6
 - elements, 45–47

- XML documents (*cont.*)
 - eliminating naming conflicts, 55
 - entities, 43
 - human-legible and clear, 6
 - internal entities, 62
 - logical structure, 37, 43–55
 - markup, 70
 - non-Unicode character codes, 38
 - physical structure, 37, 43, 60–63
 - prolog, 37, 70
 - reading, 39–40
 - structure, 43
 - text, 38
 - Unicode, 38
 - valid, 39, 42–43
 - well-formed, 39, 71
 - XML markup, 38
- XML elements, 359–361
- XML Encryption, 343–344, 378, 460
 - explicit interoperability testing, 437
 - KeyInfo element, 295
 - RetrievalMethod element, 306
 - syntax, 346–358
 - versioning, 347
- XML Encryption interoperability matrix
 - Web site, 438
- XML Encryption Recommendation, 338
- XML Encryption standard, 346, 383, 397
- XML Encryption test vectors Web site, 442, 448
- XML Encryption Working Group site, 438
- xml entity, 61
- XML Key Management, 253
- XML Key Management protocol, 293
- XML Key Management system, 319–320
- XML namespaces, 55–60, 66, 353
- xml namespaces, 104
 - attribute inheritance, 188
 - attributes, 196, 205–206
 - special handling of attributes, 197
- XML *Namespaces Frequently Asked Questions* (Bourret), 59
- XML objects, general addressing of parts of, 132–143
- XML parser, 39–40
- XML preamble, 346
- xml prefix, 58
- XML processor, 39
- XML programs, 6
- XML Protocol Working Group, 160
- XML Recommendation, 36
- XML Schema advantages, 87
- XML Schema Validation, 432–433
- XML Sec Web site, 451
- XML security, standardization process, 10
- XML Security Library, 451
- XML Signature for Java, 439
- XML signatures
 - SignatureValue elements, 247
 - verifying, 376–379
- XML tags, 7
- XML Working Group, 4
- xml:base attribute, 130–132, 204
- XML-based canonicalization algorithms, 217
- XMLDSIG (XML Digital Signatures), 10, 191, 460
 - basics, 207–211
 - Canonical XML, 170
 - combining with XML encryption, 368
 - DTD context, 211–212
 - explicit interoperability testing, 437
 - KeyInfo element, 295
 - links to P3P semantics, 254–255
 - P3P use of, 257
 - RetrievalMethod element, 306
 - signature algorithms, 251
 - SOAP, 259–262
 - user-provided signature algorithms and keying information designators, 251
 - versioning, 213
 - XML Digital Signatures, 207
 - XML syntax, 209
- XMLDSIG and Canonical XML product
 - Web site, 446
- XMLDSIG applications
 - http:access scheme, 221
 - XPath, 240
- XMLDSIG elements, 209–210, 214–215, 329
- XMLDSIG interoperability matrix Web site, 437
- XMLDSIG libraries, 246
- XMLDSIG namespace, 299, 346, 351, 425, 429
- XMLDSIG standard, 209, 245–249, 253, 300
- XMLDSIG working group, 88, 170

- XMLDSIG Working Group site, 437, 438
- xmldsig:KeyInfo element, 322, 324–327
- xmldsig:KeyName element, 330
- xmldsig:KeyValue element, 330
- xmldsig:MgmtData element, 330
- xmldsig:PGPData element, 330
- xmldsig:RetrievalMethod element, 330
- xmldsig:RetrievalMethod type, 322
- xmldsig:SPKIData element, 330
- xmldsig:X509Data element, 330
- XMLENC (XML Encryption), 10
- XMLENC WG (XML Encryption Working Group), 344
- XMLENCWG (XML Encryption Working Group), 10
- xml:lang attribute, 48–49, 121, 205
- xmlns attribute, 57
- xmlns prefix, 58
- xmlns scheme, 134
- xml:space attribute, 49–50, 82, 205
- xml:space declaration, 178
- XPath, 99, 100
 - abbreviated notation, 112, 113–114
 - applying to XML node-set, 193
 - basics, 101
 - Boolean functions, 121
 - context, 114
 - document order, 139
 - DTDs (Document Type Definitions), 102
 - equality operator, 429
 - evaluation context, 136
 - expression evaluation, 425–430
 - expressions, 112–117
 - extending, 132–143
 - function library, 117–122, 140–143
 - handling more general locations, 135
 - here() function, 428
 - location paths, 107–112
 - locations, 135–136
 - location-sets, 135–136
 - node tests, 110, 137, 138
 - node-set functions, 117–119
 - node-sets, 101, 192–193, 378–379, 426
 - number functions, 122
 - point type, 136–137
 - range types, 137–138
 - searching on and matching exact prefix names, 190
- SOAP, 261
- string functions, 119–120
- transform evaluation, 427
- transform example, 428–430
- transform input, 426
- transform output, 426–427
- transforms, 239–245
- union operator (|), 429
- XML declaration, 102
- XMLDSIG applications, 240
- XPath algorithm, 394
- XPath applications, 192
- XPath data model, 99, 101, 190
 - attribute nodes, 104
 - comment nodes, 107
 - definitions, 240
 - element nodes, 103–104
 - extension of, 190
 - namespace nodes, 104–105
 - processing instruction nodes, 106
 - root nodes, 102–103
 - text nodes, 105–106
- XPath element, 425–426
- XPath expressions, 101, 242
- XPath extensions, 135–140
- XPath Filtering algorithms, 425–430
- XPath node-set and root node, 102–103
- XPath (XML Path Language) Version 1.0, 37
- XPath-based Transform, 248
- XPointer, 37, 99, 100, 132
 - bare names, 135
 - child sequences, 135
 - document order, 139
 - encoding, 132–133
 - expressions, 134
 - forms, 133–135
 - full, 133–134
 - functions, 140–143
 - initialization of evaluation context, 139–140
 - locating names, 135
 - namespace context, 134
 - namespace declaration, 134
 - origin of link, 141
 - same-document references, 241
 - searching on and matching exact prefix names, 190
 - special characters, 132

- XPointer (*cont.*)
 - URI encoded, 133
 - XPath extensions, 135–140
 - XPointer algorithms, 394, 431–432
 - xpointer scheme, 134
 - XPointers, 242–243
 - xs:annotation element, 96
 - xs:any element, 94–95
 - xs:attribute element, 92, 94
 - xs:element element, 91, 94
 - xs:group element, 94
 - xs:import element, 96
 - xs:include element, 95
 - XSL (Extensible Stylesheet Language), 37, 65–67
 - XSL namespace, 66
 - XSLT (XSL Transformations), 100
 - apply-templates command, 427
 - searching on and matching exact prefix names, 190
 - Version 1.0, 37
 - XSLT algorithm, 394
 - XSLT Transform algorithms, 430–431
 - xs:redefine element, 96
 - xs:schema element, 91–92, 95
 - XTASS (XTML Trust Assertion Service Specification), 11
- Z**
- Zero key, 31–32